

EXHIBIT 3

SIMMONS HANLY CONROY, LLC
Jason 'Jay' Barnes (admitted *pro hac vice*)
An Truong (admitted *pro hac vice*)
Eric Johnson (admitted *pro hac vice*)
112 Madison Avenue, 7th Floor
New York, NY 10016
Telephone: (212) 784-6400
Facsimile: (212) 213-5949
jaybarnes@simmonsfirm.com
atruong@simmonsfirm.com
ejohnson@simmonsfirm.com

KIESEL LAW LLP

Jeffrey A. Koncious, State Bar No. 189803
Nicole Ramirez, State Bar No. 279017
8648 Wilshire Boulevard
Beverly Hills, CA 90211-2910
Telephone: (310) 854-4444
Facsimile: (310) 854-0812
koncious@kiesel.law

**SCOTT+SCOTT ATTORNEYS AT LAW
LLP**

Hal D. Cunningham (Bar No. 243048)
600 W. Broadway, Suite 3300
San Diego, CA 92101
Telephone: (619) 233-4565
Facsimile: (619) 233-0508
hcunningham@scott-scott.com

LOWEY DANNENBERG, P.C.

Christian Levis (admitted *pro hac vice*)
Amanda Fiorilla (admitted *pro hac vice*)
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Facsimile: (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com

**LIEFF CABRASER HEIMANN
& BERNSTEIN, LLP**

Michael W. Sobol, State Bar. No. 194857
Melissa Gardner, State Bar No. 289096
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: (415) 956-1000
Facsimile: (415) 956-1008
msobol@lchb.com
mgardner@lchb.com

**LIEFF CABRASER HEIMANN
& BERNSTEIN, LLP**

Douglas Cuthbertson (admitted *pro hac vice*)
250 Hudson Street, 8th Floor
New York, NY 10013
Telephone: 212 355-9500
Facsimile: 212-355-9592
dcuthbertson@lchb.com

Attorneys for Plaintiffs and the Proposed Class

**Additional counsel listed on signature page*

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION**

JOHN DOE I, et al. on behalf of themselves and all
others similarly situated,

Plaintiffs,

v.

GOOGLE LLC,

Defendant.

This document applies to: All Actions

Case No. 3:23-cv-02431-VC
Consolidated with: 3:23-cv-02343-VC

CLASS ACTION

****REDACTED****

**FIRST AMENDED CONSOLIDATED
CLASS ACTION COMPLAINT**

DEMAND FOR JURY TRIAL

Judge: Hon. Vince Chhabria
Action Filed: May 12, 2023

Trial Date: Not Set

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. JURISDICTION, VENUE, AND ASSIGNMENT	6
III. PARTIES	7
IV. FACTUAL ALLEGATIONS	18
A. The Health Information at Issue	18
B. How Google Unlawfully Tracks and Collects Patients' Health Information	20
1. The Google Source Code	20
a. Google Analytics	21
b. Google Ads	32
c. Google Display Ads	37
d. Google Tag and Tag Manager, Firebase SDK, Google APIs and YouTube	41
2. Google's Offline Acquisition of Health Information	44
C. Google Is Not Just a "Vendor"	46
D. How Google Monetizes the Health Information	47
1. Google's Monetization of Health Information for Remarketing Across Google's Marketing Channels	49
2. Google's Use of Health Information for Targeted Ads on Non-Google Websites and Apps	52
E. The Scope and Scale of Google's Tracking and Acquisition of Health Information	55
1. Google Source Code Is Present on 91 Percent of Health Care Provider Properties	55
2. Google Connects Health Information Across Its Advertising Systems, Google Products and Google Properties	55
3. Google's Tracking and Collection of Health Information Through the At-Issue Advertising Systems Are Connected Across Patient Devices	62
F. Google Is Reasonably Capable of – and Does – Associate the Collected Health Information to Individual Patient Identifiers	66
G. Google Can Identify the Health Care Providers From Which It Unlawfully Acquired Health Information	69

TABLE OF CONTENTS
(continued)

	Page
H. Google's Acquisition and Its Own Use of Health Information Is Unlawful and Violates Reasonable Expectations of Privacy	77
1. Google's Conduct Is Unlawful and Individuals Have a Reasonable Expectation of Privacy Under Federal Law	78
2. Google's Conduct Is Unlawful and Individuals Have a Reasonable Expectation of Privacy Under State Laws	86
3. Google's Conduct Is Unlawful and Individuals Have a Reasonable Expectation of Privacy Under Common Law	90
I. Google's Conduct Violates Its Own Express Promises	91
1. The Google Terms of Service	92
2. The Express Promises in Google Policy Documents	96
3. Google Violates These Promises	105
J. Google Acknowledges that Google Analytics Is Not Appropriate for Web Properties that Deal with Protected Health Information	111
K. Google Has Not Obtained Consent from Healthcare Providers to Engage in the Specific Conduct Alleged	113
L. Internally, Google Executives Acknowledge It Does Not Obtain Actual Consent to Any of Its Surveillance, Much Less Health Surveillance	122
M. Patients' Health Information Has Actual and Measurable Monetary Value	123
1. License Value	125
2. Individuals Have a Protectable Property Interest in Their Health Information	129
V. CLASS ACTION ALLEGATIONS	131
VI. TOLLING	133
VII. CAUSES OF ACTION	134
COUNT ONE: VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT	134
COUNT TWO: VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT	140
COUNT THREE: CALIFORNIA CONSTITUTIONAL INVASION OF PRIVACY	142
COUNT FOUR: INTRUSION UPON SECLUSION	145
COUNT FIVE: VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW	148
COUNT SIX: TRESPASS TO CHATTELS	151

TABLE OF CONTENTS
(continued)

	Page
COUNT SEVEN: CALIFORNIA COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT	154
COUNT EIGHT: BREACH OF EXPRESS CONTRACT	160
COUNT NINE: BREACH OF IMPLIED CONTRACT	164
COUNT TEN: GOOD FAITH AND FAIR DEALING	166
COUNT ELEVEN: UNJUST ENRICHMENT UNDER CALIFORNIA COMMON LAW	168
COUNT TWELVE: CONVERSION	172
VIII. PRAYER FOR RELIEF	173
IX. DEMAND FOR JURY TRIAL	177

I. INTRODUCTION

1. This case concerns Google LLC’s (“Google”) unlawful tracking, collection, and monetization of Americans’ private health information from Health Care Provider¹ web properties² in the United States, which, in a random analysis of 5,297 Health Care Providers’ web properties reveals that Google is unlawfully obtaining health information on 91% of these web properties.

2. As detailed herein, the private health information at issue includes an individual’s status as a patient of a Health Care Provider, unique patient identifiers, the specific actions taken by patients on their Health Care Provider web properties (e.g., when a patient logs in and logs out of an online patient portal, requests an appointment, or seeks information about a specific doctor, condition, treatment, or prescription drug, including specific time and frequency of each patient interaction), and content of communications that patients exchange with their Health Care Providers (“Health Information”). Content information, in turn, includes information pertaining to patient registrations, access to, and communications with their Health Care Provider within authenticated webpages (i.e. webpages that require log-in or other authentication, such as a patient portal), as well as content information pertaining to patient access to and communications with their Health Care Provider on unauthenticated web pages (e.g., communications relating to specific doctors, appointment requests, symptoms, conditions, treatments, insurance, and prescription drugs).

3. All of this Health Information is tracked and collected by Google, which, in turn, allows Google to individually identify patients, their households and their communications.

¹ As used in this Complaint, the phrase “Health Care Provider” includes all health care providers, covered entities, and business associates whose information is protected by the Health Insurance Portability and Accountability Act (“HIPAA”) or the California Confidentiality of Medical Information Act (“CMIA”). See 45 C.F.R. § 160.103; Cal. Civ. Code § 56. This includes doctors, clinics, psychologists, dentists, chiropractors, nursing homes, pharmacies, health insurance companies, pharmaceutical companies, and business associates such as vendors Cerner and Epic that operate online patient portals. *See id.*

² Web properties, as used herein, means all webpages and applications accessible via the Internet.

4. Although Google's unauthorized surveillance alone is an actionable wrong, Google also uses the collected Health Information for numerous marketing purposes, including but not limited to building short- or long-term health-related user profiles by assigning patients and their communications to specific targeting categories called "verticals"; following patients around the Internet to stalk them with future ads through a process called "remarketing"; tracking and reporting specific "conversion" events to accrue unearned revenue by keeping tabs on specific patient communications (such as an action to create an appointment, login to a patient portal, or exchange communications about a specific condition or treatment); using the collected Health Information to improperly improve its search algorithms, ad-targeting capabilities, and machine learning models; and, through Google Tag Manager, contemporaneously sharing Health Information with other tracking companies.

5. Google's unlawful tracking, collection and monetization (i.e. its internal use and profiting) of Health Information occurs through the Google Source Code³ secretly embedded in Health Care Provider web properties, which effectively tags and tracks patients visiting those sites. Almost immediately upon visiting such a web property, Google Source Code hidden in the website deposits and accesses Google tracking software, called a cookie, on the patient's device. Google designs some of their cookies to be disguised as "first-party cookies," i.e., they appear to belong to the Health Care Provider with which the patient is directly communicating. In truth, these cookies belong to Google, an unknown third party to the patient's communications with their Health Care Provider, allowing Google to track the patient surreptitiously as they navigate their Health Care Providers' web property and to intercept and redirect the patient's Health Information to Google (i.e., identifiers, actions and content of communications with their Health Care Provider).

³ Google Source Code as used herein, means the source codes associated with Google's advertising systems and products, including but not limited to the source code associated with: (1) Google Analytics; (2) Google Ads; (3) Google Display Ads; and (4) Google Tag and Tag Manager, Firebase SDK, Google APIs and YouTube.

6. By way of example, when a patient visits a Health Care Provider's web property and searches for a particular doctor to treat their condition – e.g., cardiac specialist within their area – with whom they wish to book an appointment, the patient is communicating with their Health Care Provider. But, where the Google Source Code is present, the Google Source Code causes the interception of the patient's identifiers, along with the communications content – i.e., the name of the specific doctor, condition or treatment, with whom or for which the patient wants to book an appointment – and will transmit that information to Google properties, such as Google Analytics, Google Ads and Google Display Ads. Likewise, when a patient logs in to their patient portal they are making a communication with their Health Care Provider and confirming their status as a patient of the hospital. But, where the Google Source Code is present, the Google Source Code causes the interception and transmission of the patient's identifiers, along with the specific action taken – the act of logging in to the patient portal – to Google (in many instances, this information is also accompanied by the exact date and time of log-ins and log-outs).

7. Upon receipt of this unlawfully obtained Health Information, Google uses the information for marketing in its advertising systems and products, which include but are not limited to: Google Analytics, Google Ads, Google Display Ads, Google Tag and Tag Manager, Google Firebase SDK, Google APIs, and YouTube. As detailed below, while each of these systems and products operates individually on the front end to collect Health Information, on the back end (i.e., once within Google's systems), Google connects and aggregates the Health Information, along with other information that Google has acquired about individuals. In doing so, Google is able to amplify the knowledge and insight it has about patients, compile detailed and precise profiles on patients, and monetize that information into advertising revenue. Indeed, given Google's "omnipresent surveillance" of Americans, its ability to profile individuals is unmatched.⁴

⁴ Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights*, AMNESTY INT'L 1, at 5-6 (Nov. 21, 2019), <https://www.amnesty.org/en/documents/po130/1404/2019/en/> (opining that Google and other companies engage in a "surveillance-based business model" that, among other things is "an assault on the right to privacy on an unprecedented scale") (last visited Nov. 13, 2023).

8. The Google Source Code is deployed on most Health Care Provider web properties, making it virtually impossible for patients to avoid tracking and data collection by Google when they schedule a medical appointment, make an online inquiry about an ongoing sensitive medical condition, or request prescribed medication.

9. Google's tracking, collection and monetization of patients' Health Information is in violation of federal, state, and common law that provide strict protections and safeguards regarding the inherently private and sensitive nature of this information. In fact, Google publicly admits that the federal rules on health information privacy apply to its advertising products, and that its products are inappropriate to track, collect, and monetize Americans' health information.⁵

10. Even if one puts aside the federal and state law requirements, Google's own terms of service and privacy policy assure users of all Google products that it will not collect Health Information without users' consent. And, as detailed below, Google assures users that it will comply with applicable laws, that it will not collect Health Information without consent, and that it will not use that information, or allow others to use it, for purposes of personalized advertising. Through the Google Source Code, Google routinely and systematically violates its promises.

///

///

///

///

///

///

///

///

⁵ See, e.g. Ex. 1, *HIPAA and Google Analytics*, GOOGLE ANALYTICS HELP, at 1-2, <https://support.google.com/analytics/answer/13297105> (explaining that Google Analytics is not appropriate on webpages "likely to be HIPAA-covered"). Citations herein to "Ex." are to Exhibits 1-55 attached hereto and listed in the enclosed Appendix.

11. Google's own generative AI, Google Bard, confirms the impropriety of its conduct:

The image shows two responses from Google Bard. The first response is about Google Analytics on a hospital website. It states that Google Analytics is not appropriate due to HIPAA regulations, which protect patient privacy. It suggests using a HIPAA-compliant tool like Fathom or Plausible Analytics. The second response is about Google Analytics on a company website covered by the CMIA. It states that Google Analytics is not appropriate due to CMIA regulations, which protect medical information. It suggests using a CMIA-compliant tool like Fathom or Plausible Analytics. Both responses include social sharing buttons for Facebook, Twitter, and Google, and a 'Google it' button.

Is Google Analytics appropriate on a website for a hospital covered by HIPAA?

Google Analytics is not appropriate on a website for a hospital covered by HIPAA. HIPAA is a set of regulations that protect the privacy and security of patient health information. Google Analytics collects data about website visitors, including their IP addresses. IP addresses can be used to identify individuals, which is a violation of HIPAA regulations.

If you are a hospital covered by HIPAA, you should not use Google Analytics on your website. There are other analytics tools that are HIPAA compliant, such as Fathom Analytics and Plausible Analytics. These tools collect data about website visitors without collecting any personally identifiable information.

Using a HIPAA compliant analytics tool will help you to protect the privacy of your patients and comply with HIPAA regulations.

Is Google Analytics appropriate on a website from a company covered by the California Medical Information Act?

View other drafts

Google Analytics is not appropriate on a website from a company covered by the California Medical Information Act (CMIA). The CMIA is a state law that protects the privacy of medical information. Google Analytics collects data about website visitors, including their IP addresses. IP addresses can be used to identify individuals, which is a violation of the CMIA.

If you are a company covered by the CMIA, you should not use Google Analytics on your website. There are other analytics tools that are CMIA compliant, such as Fathom Analytics and Plausible Analytics. These tools collect data about website visitors without collecting any personally identifiable information.

Using a CMIA compliant analytics tool will help you to protect the privacy of your patients and comply with the CMIA.

In addition to the above, here are some other things to consider when using Google Analytics on a healthcare website:

- Make sure that you have a privacy policy in place that clearly explains how you are collecting and using website visitor data.
- Give website visitors the option to opt out of data collection.
- Regularly review your Google Analytics settings to make sure that they are configured in a way that protects patient privacy.

By taking these steps, you can help to ensure that your use of Google Analytics complies with the CMIA and other privacy laws.

12. Plaintiffs bring this action on behalf of themselves and others similarly situated, including Google Account Holders and Non-Google Account Holders,⁶ to hold Google accountable for its unlawful tracking, collection, and monetization of patient Health Information.⁷

⁶ A Google Account Holder, as used herein, is any natural person who signed up for or was otherwise registered for a Google Account.

⁷ This action pertains to Google's tracking, acquisition, and its internal use of Health Information. It does not pertain to the sharing or sale of information to third parties through Google's Real-Time Bidding system. The Google Real-Time bidding system is the subject of an unrelated suit: *In re Google RTB Consumer Privacy Litigation*, Case No. 21-cv-02155-YGR-VKD (N.D. Cal.) (currently pending).

II. JURISDICTION, VENUE, AND ASSIGNMENT

13. This Court has personal jurisdiction over Defendant Google LLC (“Defendant” or “Google”) because it is headquartered in this District and Google consents to it in its current and prior Google Terms of Service. Further, Google designed, contrived and effectuated its scheme to track, collect and monetize Plaintiffs’ and Class Members’ Health Information from the State of California, and Google maintains and/or oversees systems designed to effectuate this scheme within the State of California.

14. Venue is proper in this District, because Google is headquartered here and because its current and prior Terms of Service purport to bind Plaintiffs and Class Members to bring disputes in this District.

15. Assignment of this case to the San Jose Division was proper pursuant to Civil Local Rule 3-2(e) because a substantial part of the events or omissions giving rise to Plaintiffs’ claims occurred in Santa Clara County, California. These consolidated actions have properly been reassigned to the San Francisco Division pursuant to pursuant to Civil Local Rule 3-12(f).

16. This Court has subject matter jurisdiction over the federal claims in this action.

17. This Court has subject matter jurisdiction over this entire action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a class action in which the amount in controversy exceeds \$5,000,000, and at least one member of the class is a citizen of a state other than the state in which Google maintains its headquarters (California) and in which it is incorporated (Delaware).

18. This Court has supplemental jurisdiction over the state law claims in this action pursuant to 28 U.S.C. § 1337, because the state law claims form part of the same case or controversy as those that give rise to the federal claims.

19. This Court has equitable jurisdiction to entertain claims and award remedies that are equitable in nature because Plaintiffs lack an adequate remedy at law. Monetary damages cannot make Plaintiffs whole for the totality of the harm to privacy rights, rights to dignity, rights to self-determination and rights to control access and use of their Health Information, or for the

harm to societal and personal expectations of privacy and justice violated by Google's conduct alleged herein. Monetary damages cannot make Plaintiffs whole for the harms caused by Google's alleged violations of statutes which do not provide for private rights of action, or for Google's alleged violations of laws which limit their application to particular aspects of the broad-ranging pattern of activity by Google alleged herein. Further, there is no adequate remedy at law and an award of damages under the law will not necessarily encompass profits or benefits Google unjustly earned as a result of its unauthorized post-collection use of Plaintiffs' and Class Members' Health Information, which it may not retain under California law. Additionally, Plaintiffs may be unable to obtain full relief on a class-wide basis under each legal claim and/or on behalf of a certified Class due to different requirements of proof (e.g., mens rea and reliance) and the Court may permit Plaintiffs to plead both damages and, in the alternative, equitable remedies at the early pleadings stage. In addition, the Court has equitable jurisdiction to issue injunctions that serve different purposes and remedy different harms than retrospective monetary damages.

III. PARTIES

20. Plaintiff **John Doe I** is a resident of Wisconsin and a patient of Gundersen Health System ("Gundersen"). Gundersen owns and operates hospitals and clinics in Wisconsin, Minnesota and Iowa, and owns and operates a web property, which includes www.gundersenhealth.org and a patient portal at mychart.gundersenhealth.org. John Doe I exchanged communications about his care (including his conditions, treatments, and providers), with his Health Care Provider, Gundersen, on the Gundersen web property. John Doe I had a reasonable expectation that Google would not track, collect, or monetize the Health Information he exchanged with his Health Care Provider. Nonetheless, without his knowledge or consent, Google tracked, collected, and monetized his Health Information exchanged with his Health Care Provider. Upon information and belief, Google tracked, collected, and monetized John Doe I's Health Information exchanged with his Health Care Provider on the Gundersen web property through, among other things, the Google Source Code. The full scope of Google's interceptions of

John Doe I's communications with Gundersen, including the detailed URLs, identifiers and other communication are solely within Google's possession. Investigation reveals that Google intercepted and shared without authorization at least the following information about John Doe I's communications on the Gundersen web property: communications about his log-ins to the Gundersen patient portal; communications related to doctor searches specific to his medical needs, including searches for a [REDACTED]; communications about when he views medical records, medications, and lab results within the patient portal; communications about his Health Care Providers, including [REDACTED] [REDACTED]; and communications about his specific conditions or treatments, including [REDACTED]
[REDACTED]

21. Plaintiff **John Doe II** is a resident of California and a patient of Kaiser Permanente ("Kaiser"). Kaiser owns and operates hospitals and clinics in California, Colorado, Georgia, Hawaii, Maryland, Virginia, Washington D.C., Oregon, and Washington, and owns and operates a web property, which includes www.kaiserpermanente.org and a patient portal at <https://healthy.kaiserpermanente.org/consumer-sign-on#/signon>. John Doe II exchanged communications about his care (including his conditions, treatments, providers, and appointments), with his Health Care Provider, Kaiser, on the Kaiser web property. John Doe II had a reasonable expectation that Google would not track, collect, or monetize the Health Information he exchanged with his Health Care Provider. Nonetheless, without his knowledge or consent, Google tracked, collected, and monetized his Health Information exchanged with his Health Care Provider. Upon information and belief, Google tracked, collected, and monetized John Doe II's Health Information exchanged with his Health Care Provider on the Kaiser web property through, among other things, the Google Source Code. The full scope of Google's interceptions of John Doe II's communications with Kaiser, including the detailed URLs, identifiers and other sources of communication are solely within Google's possession. Investigation reveals that Google intercepted and shared without authorization at least the following information about John Doe

II's communications on the Kaiser web property: communications related to doctor searches specific to his medical needs, including searches for a [REDACTED]; communications about payment of bills; communications about scheduling of appointments; communications about his log-ins to the Kaiser patient portal; communications about when he views medical records, medications, and lab results within the patient portal; communications about his doctors, including [REDACTED] [REDACTED]; and communications about his specific conditions or treatments, including [REDACTED].

22. Plaintiff **John Doe III** is a resident of Illinois and a patient of Rush University System for Health (“Rush”). Rush operates over 300 hospitals and clinics in Illinois, and owns and operates a web property, which includes <https://www.rush.edu/> and a patient portal at <https://mychart.rush.edu/mychart/Authentication/Login?>. John Doe III exchanged communications about his care (including his conditions, treatments, providers, and appointments), with his Health Care Provider, Rush, on the Rush web property. John Doe III had a reasonable expectation that Google would not track, collect, or monetize the Health Information he exchanged with his Health Care Provider. Nonetheless, without his knowledge or consent, Google tracked, collected, and monetized his Health Information exchanged with his Health Care Provider. Upon information and belief, Google tracked, collected, and monetized John Doe III’s Health Information exchanged with his Health Care Provider on the Rush web property through, among other things, the Google Source Code. The full scope of Google’s interceptions of John Doe III’s communications with Rush, including the detailed URLs, identifiers and other sources of communication are solely within Google’s possession. Investigation reveals that Google intercepted and shared without authorization at least the following information about John Doe III’s communications on the Rush web property: communications about his log-ins to the Rush patient portal; communications about scheduling appointments; communications related to doctor searches specific to his medical needs, including a primary care provider; communications about when he views his medical records, medications, and lab results within the patient portal; communications about his healthcare providers, including [REDACTED]

████████; and communications about the patient and his specific conditions or treatments, including
████████.

23. Plaintiff **John Doe IV** is a resident of California and a patient of Kaiser Permanente (“Kaiser”). Kaiser owns and operates hospitals and clinics in California, Colorado, Georgia, Hawaii, Maryland, Virginia, Washington D.C., Oregon, and Washington, and owns and operates a web property, which includes www.kaiserpermanente.org and a patient portal at <https://healthy.kaiserpermanente.org/consumer-sign-on#/signon>. John Doe IV exchanged communications about his care (including his conditions, treatments, providers, and appointments), with his Health Care Provider, Kaiser, on the Kaiser web property. John Doe IV had a reasonable expectation that Google would not track, collect, or monetize the Health Information he exchanged with his Health Care Provider. Nonetheless, without his knowledge or consent, Google tracked, collected, and monetized his Health Information exchanged with his Health Care Provider. Upon information and belief, Google tracked, collected, and monetized John Doe IV’s Health Information exchanged with his Health Care Provider on the Kaiser web property through, among other things, the Google Source Code. The full scope of Google’s interceptions of John Doe IV’s communications with Kaiser, including the detailed URLs, identifiers and other sources of communication are solely within Google’s possession. Investigation reveals that Google intercepted and shared without authorization at least the following information about John Doe IV’s communications on the Kaiser web property: communications about his log-ins to the Kaiser patient portal; communications related to doctor searches specific to his medical needs, including searches for a primary care provider; communications about scheduling of appointments; communications about when he views medical records, test results, and visit summaries within the patient portal; communications about his doctors, including [REDACTED]

[REDACTED]; and communications about his specific conditions or treatments, including [REDACTED]

[REDACTED]

24. Plaintiff **John Doe V** is a resident of Florida and a patient of Tallahassee Memorial HealthCare. Tallahassee Memorial HealthCare owns and operates a hospital and clinics in Florida, and owns and operates a web property, which includes <https://www.tmh.org/> and two patient portals <https://www.followmyhealth.com/bookmark#/default> and <https://tmh.consumeridp.us-1.healtheintent.com/saml2/sso/login?authenticationRequestId=b1b5d76a-d605-47cf-95cf-c589900a186a>. John Doe V exchanged communications about his care (including his conditions, treatments, providers, and appointments), with his Health Care Provider, Tallahassee Memorial HealthCare, on the Tallahassee Memorial HealthCare web property. John Doe V had a reasonable expectation that Google would not track, collect, or monetize the Health Information he exchanged with his Health Care Provider. Nonetheless, without his knowledge or consent, Google tracked, collected, and monetized his Health Information exchanged with his Health Care Provider. Upon information and belief, Google tracked, collected, and monetized John Doe V's Health Information exchanged with his Health Care Provider on the Tallahassee Memorial HealthCare web property through, among other things, the Google Source Code. The full scope of Google's interceptions of John Doe V's communications with Tallahassee Memorial HealthCare, including the detailed URLs, identifiers and other sources of communication are solely within Google's possession. Investigation reveals that Google intercepted and shared without authorization at least the following information about John Doe V's communications on the Tallahassee Memorial HealthCare web property: communications related to doctor searches specific to his medical needs, including searches for a [REDACTED]; communications about viewing bills; communications about his log-ins to the Tallahassee Memorial HealthCare patient portal; communications about when he views medical records, medications, lab results, and visit summaries within the patient portal; communications about his doctors, including [REDACTED]; and communications about his specific conditions or treatments including his [REDACTED].

25. Plaintiff **Jane Doe I** is a resident of Maryland and a patient of Health Care Provider MedStar Health ("MedStar") and Mercy Medical Center, Baltimore, MD ("Mercy MD"). MedStar owns and operates hospitals and clinics in Maryland, Washington D.C., and Virginia, and owns

and operates a web property, which includes www.medstarhealth.org and a patient portal at www.medstarhealth.org/mymedstar-patient-portal. Mercy MD owns and operates hospitals and clinics in Maryland, and owns and operates a web property, which includes www.mdmercy.com and a patient portal at <https://mychart.mdmercy.com/mychart/Authentication/Login>. Jane Doe I exchanged communications about her care (including her conditions, treatments, providers, and appointments) with her Health Care Providers, MedStar and Mercy MD, on their web properties. Jane Doe I had a reasonable expectation that Google would not track, collect, or monetize the Health Information she exchanged with her Health Care Providers. Nonetheless, without her knowledge or consent, Google tracked, collected, and monetized her Health Information exchanged with her Health Care Providers. Upon information and belief, Google tracked, collected, and monetized Jane Doe I's Health Information exchanged with her Health Care Providers on the MedStar and Mercy MD web properties through, among other things, the Google Source Code. The full scope of Google's interceptions of Jane Doe I's communications with MedStar and Mercy MD, including the detailed URLs, identifiers and other sources of communication are solely within Google's possession. Investigation reveals that Google intercepted and shared without authorization at least the following information about Jane Doe I's communications on the MedStar and Mercy MD web properties: communications related to doctor searches specific to her medical needs, including searches for a [REDACTED]; communications about payment of bills; communications about her log-ins to the MedStar and Mercy MD patient portals; communications about when she views medical records and lab results within the patient portal; and communications about her specific conditions or treatments, including [REDACTED].

26. Plaintiff Jane Doe II is a resident of Illinois and a patient of OSF St. Anthony Medical Center – OSF HealthCare (“OSF”) and Alton Memorial Hospital – BJC Healthcare (“Alton Memorial”). OSF owns and operates hospitals and clinics in Illinois and Michigan, and owns and operates a web property, which includes www.osfhealthcare.org and a patient portal at www.osfhealthcare.org/mychart. BJC Healthcare owns and operates hospitals and clinics in

Illinois and Missouri, and owns and operates a web property, which includes www.altonmemorialhospital.org and a patient portal at www.bjc.org/mychart. Jane Doe II exchanged communications about her care (including her conditions, treatments, providers, and appointments) with her Health Care Providers, OSF and Alton Memorial, on the Health Care Providers' web properties. Jane Doe II had a reasonable expectation that Google would not track, collect, or monetize the Health Information she exchanged with her Health Care Providers. Nonetheless, without her knowledge or consent, Google tracked, collected, and monetized her Health Information exchanged with her Health Care Providers. Upon information and belief, Google tracked, collected, and monetized Jane Doe II's Health Information exchanged with her Health Care Providers on the OSF and Alton Memorial web properties, among other things, the Google Source Code. The full scope of Google's interceptions of Jane Doe II's communications with OSF and Alton Memorial, including the detailed URLs, identifiers and other sources of communication are solely within Google's possession. Investigation reveals that Google intercepted and shared without authorization at least the following information about Jane Doe II's communications on the OSF and Alton Memorial web properties: communications related to doctor searches specific to her medical needs, including searches for a [REDACTED] and primary care provider; communications about payment of bills; communications about scheduling of appointments; communications about her log-ins to the OSF and Alton Memorial patient portals; communications about when she views medical records, medications, and lab results within the patient portal; communications about his doctors, including [REDACTED] [REDACTED]; and communications about his specific conditions or treatments, including [REDACTED]

27. Plaintiff **Jane Doe III** is a resident of Nevada and a patient of Health Care Provider Kaiser and insured by United Health Care ("UHC"). Kaiser owns and operates hospitals and clinics in California, Colorado, Georgia, Hawaii, Maryland, Virginia, Washington D.C., Oregon, and Washington, and owns and operates a web property, which includes www.kaiserpermanente.org and a patient portal at <https://healthy.kaiserpermanente.org/consumer-sign-on#/signon>. UHC owns and operates a web property at www.uhc.com. Jane Doe III exchanged communications about her

care (including her conditions, treatments, and providers) with her Health Care Providers, Kaiser and UHC, on their respective web properties. Jane Doe III had a reasonable expectation that Google would not track, collect, or monetize the Health Information she exchanged with her Health Care Providers. Nonetheless, without her knowledge or consent, Google tracked, collected, and monetized her Health Information she exchanged with her Health Care Providers. Upon information and belief, Google tracked, collected, and monetized Jane Doe III's Health Information exchanged with her Health Care Providers on the Kaiser and UHC web properties through, among other things, the Google Source Code. The full scope of Google's interceptions of Jane Doe III's communications with Kaiser and UHC, including the detailed URLs, identifiers and other sources of communication are solely within Google's possession. Investigation reveals that Google intercepted and shared without authorization at least the following information about Jane Doe III's communications on the Kaiser and UHC web properties: communications about payment of bills; communications about scheduling of appointments; communications about her log-ins to the Kaiser and UHC patient portals; communications about when she views medical records, medications, and lab results within the patient portal; communications about her Health Care Providers, including [REDACTED]; and communications about her specific conditions or treatments, including [REDACTED]

28. Plaintiff Jane Doe IV is a resident of Maryland and a patient of Health Care Provider MedStar. MedStar owns and operates hospitals and clinics in Maryland, Washington D.C., and Virginia, and owns and operates a web property, which includes www.medstarhealth.org and a patient portal at www.medstarhealth.org/mymedstar-patient-portal. Jane Doe IV exchanged communications about her care (including her conditions, treatments, providers, and appointments) with her Health Care Provider, MedStar, on the MedStar web property. Jane Doe IV had a reasonable expectation that Google would not track, collect, or monetize the Health Information she exchanged with her Health Care Provider. Nonetheless, without her knowledge or consent, Google tracked, collected, and monetized her Health Information exchanged with her Health Care Provider. Upon information and belief, Google tracked, collected, and monetized Jane

Doe IV's Health Information exchanged with her Health Care Provider on the MedStar web property through, among other things, the Google Source Code. The full scope of Google's interceptions of Jane Doe IV's communications with MedStar, including the detailed URLs, identifiers and other sources of communication are solely within Google's possession. Investigation reveals that Google intercepted and shared without authorization at least the following information about Jane Doe IV's communications on the MedStar web property: communications about scheduling of appointments; communications about her log-ins to the MedStar patient portal; and communications about when she views medical records, medications, and/or lab results within the patient portal.

29. Plaintiff Jane Doe V is a resident of California and a patient of Planned Parenthood Burbank Health Center. Planned Parenthood Burbank Health Center is operated by Planned Parenthood Los Angeles, which is an affiliate of Planned Parenthood Federation of America that owns and operates a web property, which includes <https://www.plannedparenthood.org> and <https://www.plannedparenthood.org/health-center>. Jane Doe V exchanged communications about her care (including her conditions and treatments), with her Health Care Provider, Planned Parenthood Federation of America, on the Planned Parenthood web property. Jane Doe V had a reasonable expectation that Google would not track, collect, or monetize the Health Information she exchanged with her Health Care Provider. Nonetheless, without her knowledge or consent, Google tracked, collected, and monetized her Health Information exchanged with her Health Care Provider. Upon information and belief, Google tracked, collected, and monetized Jane Doe V's Health Information exchanged with her Health Care Provider on the Planned Parenthood web property through, among other things, the Google Source Code. The full scope of Google's interceptions of Jane Doe V's communications with Planned Parenthood, including the detailed URLs, identifiers and other sources of communication are solely within Google's possession. Investigation reveals that Google intercepted and shared without authorization at least the following information about Jane Doe V's communications on the Planned Parenthood web

property: communications related to the specific procedure she was seeking, including [REDACTED] and communications related to facility searches specific to her medical needs, including [REDACTED].

30. Plaintiff Jane Doe VI is a resident of Texas and a patient of Shannon Medical Center. Shannon Medical Center owns and operates hospitals and clinics in Texas, and owns and operates a web property, which includes <https://www.shannonhealth.com/> and <https://www.shannonhealth.com/patients-and-visitors/patient-portal-mychart/>. Jane Doe VI exchanged communications about her care (including her conditions, medications, treatments, providers, and appointments), with her Health Care Provider, Shannon Medical Center, on the Shannon Medical Center web property. Jane Doe VI had a reasonable expectation that Google would not track, collect, or monetize the Health Information she exchanged with her Health Care Provider. Nonetheless, without her knowledge or consent, Google tracked, collected, and monetized her Health Information exchanged with her Health Care Provider. Upon information and belief, Google tracked, collected, and monetized Jane Doe VI's Health Information exchanged with her Health Care Provider on the Shannon Medical Center web property through, among other things, the Google Source Code. The full scope of Google's interceptions of Jane Doe VI's communications with Shannon Medical Center, including the detailed URLs, identifiers and other sources of communication are solely within Google's possession. Investigation reveals that Google intercepted and shared without authorization at least the following information about Jane Doe VI's communications on the Shannon Medical Center web property: communications related to doctor searches specific to her medical needs, including searches for a [REDACTED] [REDACTED] [REDACTED]; communications about scheduling of appointments; communications about her log-in to the Shannon Medical Center patient portal; communications when she viewed medical records, medications, and lab results within the patient portal; communications about her healthcare providers, including [REDACTED] [REDACTED] [REDACTED]; and communications about her [REDACTED]

specific conditions or treatments including [REDACTED]

[REDACTED].

31. Plaintiff **Jane Doe VII** is a resident of Illinois and a patient of Edward-Elmhurst Health. Edward-Elmhurst Health owns and operates hospitals and clinics in Illinois, and owns and operates a web property, which includes <https://www.eehealth.org/> and <https://mychart.eehealth.org/mychart/Authentication/Login?>. Jane Doe VII exchanged communications about her care (including her conditions, medications, treatments, providers, and appointments), with her Health Care Provider, Edward-Elmhurst Health, on the Edward-Elmhurst Health web property. Jane Doe VII had a reasonable expectation that Google would not track, collect, or monetize the Health Information she exchanged with her Health Care Provider. Nonetheless, without her knowledge or consent, Google tracked, collected, and monetized her Health Information exchanged with her Health Care Provider. Upon information and belief, Google tracked, collected, and monetized Jane Doe VII's Health Information exchanged with her Health Care Provider on the Edward-Elmhurst Health web property through, among other things, the Google Source Code. The full scope of Google's interceptions of Jane Doe VII's communications with Edward-Elmhurst Health, including the detailed URLs, identifiers and other sources of communication are solely within Google's possession. Investigation reveals that Google intercepted and shared without authorization at least the following information about Jane Doe VII's communications on the Edward-Elmhurst Health web property: communications related to doctor searches specific to her medical needs, including searches for [REDACTED] [REDACTED]; communications about scheduling of appointments; communications about her logins to the Edward-Elmhurst Health patient portal; communications about when she views medical records, medications, test and lab results within the patient portal; communications about her doctors, including [REDACTED].

32. Defendant **Google LLC** is a Delaware Limited Liability Company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, whose membership interests are entirely held by its parent holding company, Alphabet, Inc. ("Alphabet"), headquartered at the

same address. Alphabet trades under the stock trading symbols GOOG and GOOGL. Alphabet generates revenues primarily by delivering targeted online advertising through the Google subsidiary. All operations relevant to this Complaint are run by Google, who, among other things, is the creator of the Google Source Code, is an established advertising company, and knew at all times that the incorporation of the Google Source Code on Health Care Providers' web properties would result in its interception of Health Information, including information relating to patient status, appointments, treatments, conditions, and communications with Health Care Providers.

IV. FACTUAL ALLEGATIONS

A. The Health Information at Issue

33. As noted above, Google collects, tracks, uses, and monetizes Health Information that includes data identifying an individual's status as a patient of a specific Health Care Provider, unique patient identifiers, the specific actions taken by patients on their Health Care Provider web properties, and content of communications that patients exchange with their Health Care Providers.

34. Identifiers: As used in this Complaint, unique patient identifiers include but are not limited to:

- a. Names;
- b. Geolocation;
- c. Demographic information;
- d. Internet Protocol (IP) addresses;
- e. User Agent information;
- f. Device identifiers;
- g. Device qualities sufficient to uniquely identify the device;
- h. The NID cookie associated with transmissions to Google.com from non-Google websites and directly on Google.com;
- i. Google Account identifying cookies associated with transmissions to Google.com from non-Google websites and directly on Google.com;

- j. The IDE cookie associated with transmissions to Doubleclick.net (i.e., Google Display Ads) from non-Google websites;
- k. The DSID cookie associated with transmissions to Doubleclick.net from non-Google websites;
- l. The _ga, _gid, and other Google cookies associated with Google Analytics;
- m. The cid, gid, and other user or device identifying data parameters associated with Google Analytics;
- n. The Android Advertising ID, iOS Advertising Identifier (IDFA), Installation ID, and Instance ID;
- o. Any publisher provided identifier provided to Google; and
- p. Any other cookies or identifiers that permit Google to track a user across sites or devices.

35. As discussed further below, these identifiers constitute protected information under federal and California state law. *See, e.g.* HIPAA, 42 U.S.C. § 1320(6) and 45 C.F.R. 160.103; California Consumer Protection Act (CCPA), Cal. Civ. Code § 1798.140(v)(1); CMIA, Cal. Civ. Code § 56.05(i), as well as “content” of electronic communications protected under federal and state wiretap acts (*see, e.g.* Electronic Communications Protection Act, 18 U.S.C. § 2511; California Invasion of Privacy Act, Cal. Penal Code § 631).

36. Specific Actions & Content of Communications: As used in this Complaint, the specific actions taken by patients and content of communications that patients exchanged with their Health Care Providers may include and are not limited to:

- a. Website browsing history and URL information, which reveals the substance, purport, and meaning of communications between patients and their Health Care Providers, including information exchanged inside of authenticated (e.g., patient portals) and unauthenticated pages relating to Health Care Providers, services, medical appointments, medical conditions, treatments, health insurance, and more;

- b. Information which reveals the precise actions taken by the patients on their Health Care Providers' web properties, for example, the buttons clicked (such as logging in or out of a patient portal), requests for appointments made, searches undertaken, or other information requested;
- c. Medical and related information patients fill out in online forms to their Health Care Providers and related event data;
- d. Timing and frequency of patients' visits to their Health Care Providers web properties including, for example, the precise times patients log-in and out of patient portals; and
- e. Information Google collects from Health Care Providers through customer lists (explained below) that are uploaded to Google.

B. How Google Unlawfully Tracks and Collects Patients' Health Information

37. Google's unlawful tracking, collection, and monetization of patients' Health Information occurs both on web-browsers and on apps.

38. Google's unlawful tracking, collection and monetization of patient Health Information occurs primarily through the use of: (1) the Google Source Code; and (2) "offline" sources.

1. The Google Source Code

39. As noted above, Google Source Code is designed to track and collect individuals' information when they are browsing the Internet.

40. Google Source Code is provided by Google in a copy-and-paste format and its functionality is uniform on all web properties. Its operation is hidden by Google's design and does not indicate to users that Google Source Code is present on a web property or app they are using.

41. When the Google Source Code is placed on a Health Care Provider's web property, the Google Source Code commands the patient's computing device, either through the web-browser or the app, to track, intercept and redirect the patient's Health Information to Google.

42. This tracking, interception and redirection of Health Information occurs when patients are exchanging communications with their Health Care Providers using web-browsers and when they are using apps that have adopted a Google SDK or “software development kit,” which is a collection of software used in an app that has integrated the Google Source Code.

43. Upon information and belief, there are three primary Google products and services which leverage Google Source Code to track, collect and, subsequently use (i.e., monetize), individuals’ Health Information. These are: (a) Google Analytics; (b) Google Ads; and (c) Google Display Ads; as well as various other products and services, including but not limited to (d) Google Tag Manager and Google Tag, Google Firebase SDK, Google APIs, and YouTube.

44. Each of these products and services are designed for the express purpose of ingesting millions of data points from end users to provide: (1) in-depth insights about individuals in the form of analytics; (2) hyper-specific targeting of individuals through Google’s ad products; and (3) importantly, for Google, access to “first party” data it would not otherwise be privy to and from which it profits and uses for its own purposes.

a. **Google Analytics**

45. Google Analytics is a Google marketing tool, used for advertising and analytics. A fundamental and primary purpose of Google Analytics is to obtain the information about consumers’ communications and activities that is accessible by entities other than Google. Google accomplishes this through Google Analytics, in part, by touting it as a tool that enables clients to “understand the customer journey and improve marketing ROI.”⁸ Specifically, according to Google, Google Analytics is intended to help advertisers:

- a. “Unlock customer-centric measurement” to “[u]nderstand how your customers interact across your sites and apps, throughout their entire lifecycle”;

⁸ Ex. 2, *Analytics*, GOOGLE MARKETING PLATFORM, at 1,
<https://marketingplatform.google.com/about/analytics/>.

b. “Get smarter insights to improve ROI,” to “[u]ncover new insights and anticipate future customer actions with Google’s machine learning to get more value out of your data”; and

c. “Connect your insights to results,” to “[t]ake action to optimize marketing performance with integrations across Google’s advertising and publisher tools[.]”⁹

46. Google Analytics includes Universal Analytics, Google Analytics 360, Google Analytics 4, and Google Analytics for Firebase. Irrespective of what label it operates under, Google Analytics is “[d]esigned to work seamlessly with other Google solutions and partner products.”¹⁰ As discussed further below, this includes other Google marketing and advertising products, such as: Google Ads, Display & Video 360, Search Ads 360, Google Cloud, Salesforce Marketing Cloud Integration, Google Ad Manager, Google Tag, Google Firebase SDK, and Google’s AdMob SDK.

47. Google Analytics is associated with the domains www.Google-Analytics.com and analytics.google.com.

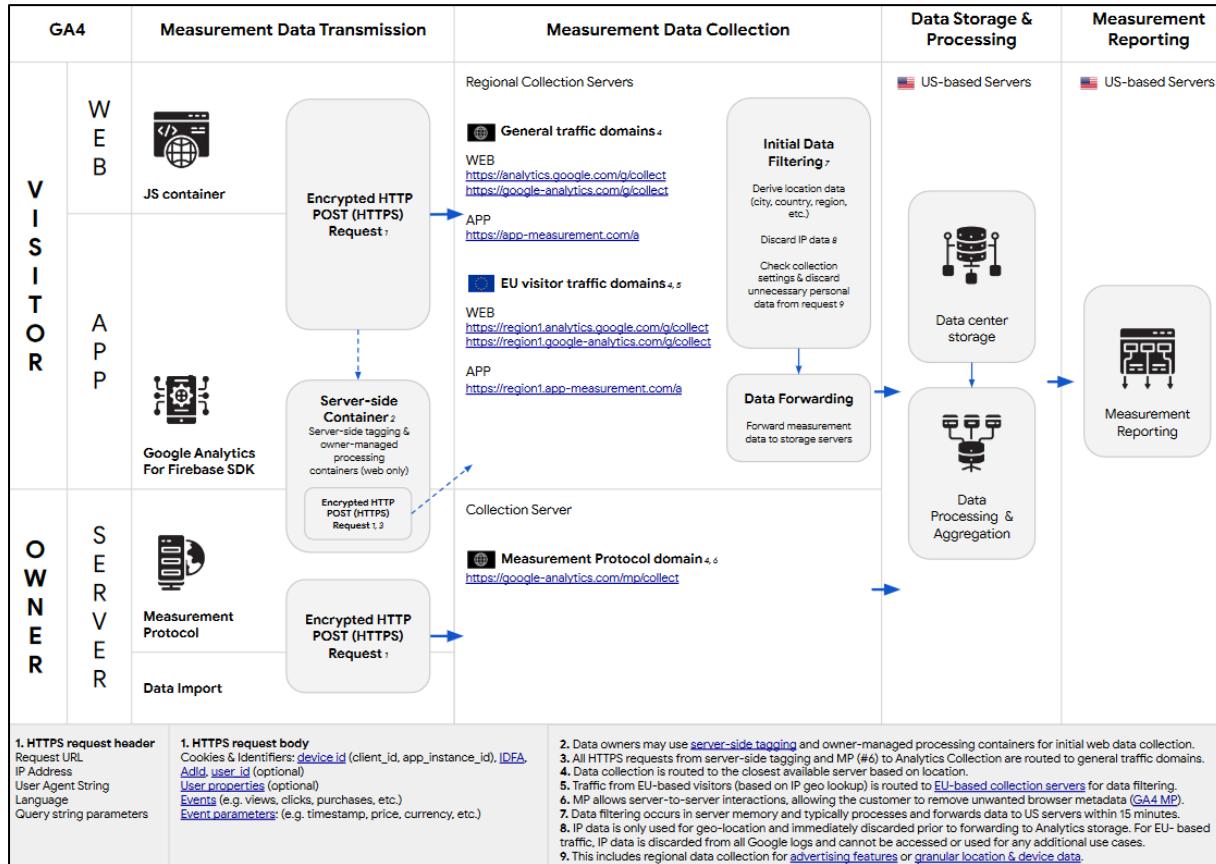
48. Upon information and belief, based on the investigation of counsel and expert analysis, the Google Source Code intercepts and redirects patient Health Information to Google Analytics on approximately 60 percent of Health Care Provider properties that were analyzed by Plaintiffs’ expert.

49. When the Google Source Code for Google Analytics is present on a Health Care Provider’s website, that source code commands patients’ communications devices to track, intercept, and send patients’ Health Information to Google.

⁹ *Id.* (Ex. 2) at 3.

¹⁰ Ex. 3, *Analytics 360*, GOOGLE MARKETING PLATFORM, at 14, <https://marketingplatform.google.com/about/analytics-360/features/#integrations>; see also Ex. 2, *supra* n.8 at 6 (products are “[d]esigned to work together”); Ex. 4, *Set up your Google tag*, GOOGLE ANALYTICS HELP, at 1, <https://support.google.com/analytics/answer/12002338> (“The Google tag sends data to connected destinations, such as Google Ads and Google Analytics”); Ex. 5, *Analytics for Firebase*, GOOGLE FIREBASE DOCUMENTATION, at 1, <https://firebase.google.com/docs/analytics> (“Analytics integrates across Firebase features”).

50. Google has published the below diagram explaining this data flow:¹¹



51. As illustrated in the above diagram, the Google Source Code causes the interception and redirection of HTTPS Requests¹² to Google Analytics. According to Google's own diagram, the redirected HTTPS request includes, among other things: "Cookies & Identifiers," which include the identifiers at issue in this action; and "Request URL" and "Query string parameters," which include the "content of communications" at issue in this action.

52. **MedStar Example.** Plaintiffs provide an explanation for each of these categories of information below using MedStar as an example.

¹¹ Ex. 6, *Safeguarding Your Data*, GOOGLE ANALYTICS HELP, <https://support.google.com/analytics/answer/6004245> ("Download this diagram that explains how Google Analytics collects, filters, and stores data").

¹² HTTPS Requests is an Internet protocol that secures communication and data transfer between an individual's web browser and the website.

53. Cookies: Cookies are small text files that are saved to web browsers for, among other things, tracking Internet users and their web browsing history. First-party cookies belong to a web property on which an individual is directly communicating and, typically, remain only on that web property. Third-party cookies originate from a web property that a user is not currently visiting. Third-party cookies are often referred to as “tracking cookies” because they exist primarily to enable third parties to track individuals as they navigate the internet and collect their personal information.

54. When a patient visits a Health Care Provider web property containing the Google Source Code for Google Analytics, that source code is designed to deposit the Google Analytics cookies, named `_ga`, `_gid` and `_gcl_au`, on the patient’s computing device. Although these cookies belong to Google (who is a third party to the communication between a patient and their Health Care Provider), the Google Analytics Source Code disguises these cookies as “first-party” cookies that belong to the Health Care Provider.

55. For example, MedStar’s web property has been embedded with the Google Source Code for Google Analytics. When a patient visits the MedStar homepage or patient portal, the Google Source Code deposits the Google Analytics cookies on to the patient’s device and designates these cookies as belonging to MedStar.

56. By disguising the Google Analytics cookies as belonging to MedStar (a first party to the communication) instead of Google (a third party to the communication), the Google Source Code is able to circumvent security measures that would prevent third-party tracking via third-party cookies. That is, a patient’s attempt to block third-party cookies would fail with respect to the Google Analytics cookies, because the Google Source Code has disguised these cookies as belonging to first party MedStar.

57. Because the Google Analytics cookies are disguised as first-party cookies they will likely not be blocked, because Health Care Providers typically require acceptance of first-party cookies for a patient to engage with their web properties, including engagement with any “authenticated” activity (e.g. patient portals) on the Health Care Providers’ web properties. For

example, for security purposes, MedStar requires that a patient’s computing device accept first-party cookies in order for a patient to access the MedStar patient portal.

58. Because the Google Source Code appears on the MedStar website, the placement of the Google Analytics cookies – and thus, the tracking of patients by Google via Google Analytics – occurs the moment that patients begin interacting with their Health Care Provider (e.g. MedStar), and it continues for almost every interaction and communication that occurs thereafter, including when a patient interacts with “authenticated” web pages, like the MedStar patient portal.

59. Identifiers: When a patient visits a Health Care Provider web property containing the Google Source Code for Google Analytics, that source code is designed to redirect to Google Analytics the patient’s device and other identifiers.

60. For example, when a patient interacts with MedStar’s web property, including its patient portal, identifiers that are intercepted by the Google Source Code and transmitted to Google Analytics may include and are not limited to:

- a. The patient’s IP address;¹³
- b. The patient’s User-Agent;¹⁴
- c. Google cookies that are disguised as first-party cookies, which include the following: _ga, _gid, and _gcl_au;
- d. URL data parameters that include identifiers named ‘cid’ and ‘gid,’ which is the method through which Google passes the values for the _ga, _gid, and _gcl_au cookie values to itself;
- e. Patient device identifiers; and
- f. Patient device attributes sufficient to uniquely identify the device under a scientific principle generally known as “entropy” to data scientists.

¹³ An IP address is a numerical identifier that identifies the patient’s network and location to direct their communications. An IP address is considered individually identifiable as a matter of law under HIPAA and the CCPA.

¹⁴ A User-Agent identifies details about the patient’s browser. When combined with an IP address, it is additional identification data to help uniquely identify a device and the person using the device.

61. Request URL: Request URLs contain information about the substance, purport, and meaning of patients' communications with their Health Care Providers. When a patient visits a Health Care Provider web property containing the Google Source Code for Google Analytics, that source code is designed to redirect to Google Analytics Request URL information that may include and is not limited to:

- a. The Request URL, and portions thereof that specifically identify doctors, conditions, treatments, services, prescription drugs, payment information, health insurance information, appointment requests, and log-in/log-out information that were the subject of communications exchanged between patients and their Health Care Providers; and
- b. Events, such as "views, clicks, purchases."

62. For example, when a patient interacts with MedStar's web property, including its patient portal, Request URLs that are intercepted by the Google Source Code and transmitted to Google Analytics may include and are not limited to:

- a. Searches for a doctor on MedStar's web property;
- b. Requests for an appointment on MedStar's web property;
- c. Search terms, results, or other communications relating to MedStar's health services, conditions, tests, and treatments, for example:

<https://www.medstarhealth.org/services/abdominal-aneurysm-treatment;>

[https://www.medstarhealth.org/services/blood-cancer-treatments;](https://www.medstarhealth.org/services/blood-cancer-treatments) and

[https://www.medstarhealth.org/services/behavioral-health-treatments;](https://www.medstarhealth.org/services/behavioral-health-treatments)

- d. Patient communications to log-in or enroll in the MedStar patient portal;
- e. Information about communications exchanged by patients after they have logged-in to the MedStar patient portal; and
- f. Patient communication to log-out of the MedStar patient portal.

63. Examples of "Events" redirected by the Google Source Code to Google Analytics on MedStar's web property may include and are not limited to:

- a. Page views about specific MedStar services, conditions, tests, and treatments;
- b. Patient portal logs-ins, enrollments, and log-outs;
- c. Appointment requests; and
- d. Search terms and results for doctors, services, conditions, tests, and treatments.

64. Query String Parameters: Query String Parameters pertain to additional information that may be included after a website's base URL and filepath.¹⁵ The types of information included are often referred to as a "field" and corresponding "value" (i.e. field=value). Query String Parameters may include and are not limited to: unique identifiers, descriptions of precise actions taken, and descriptions of the content of the page viewed.

65. When a patient visits a Health Care Provider web property where the Google Source Code for Google Analytics is present, that source code redirects Query String Parameters to Google. As explained below, Query String Parameters can reveal patients' identifiers, specific interactions with the Health Care Provider web properties, and the details and content of their communications.

66. Gundersen Example. For example, when a patient interacts with Gundersen's web property the Query String Parameters that are intercepted by Google Source Code and redirected to Google Analytics may include and are not limited to the following:

Field	Value and Explanation
	Value = Event
t	Explanation: The "t" field equals a value that describes a particular type of event. The "t" field and value can therefore identify a specific action being taken by a patient.

¹⁵ It is not necessary to the functionality of a Health Care Provider's web property for Query String Parameters to be sent to Google.

Field	Value and Explanation
	For example, t=pageview, t=screenview, t=event, t=transaction, t=item. ¹⁶
ec	<p>Value = Event Category</p> <p>Explanation: The “ec” field is equal to a value that provides further specificity as to the “event” (e.g. action) being taken by a patient. According to Google, this field “[s]pecifies the event category. Must not be empty.”¹⁷ The “ec” field and value can therefore identify a specific action being taken by a patient.</p> <p>For example, ec=user_action</p>
ea	<p>Value = Click</p> <p>Explanation: The “ea” field is equal to a value that provides further specificity as to the “event” (e.g.. action) being taken by a patient. According to Google, this field “[s]pecifies the event action. Must not be empty.”¹⁸ The “ea” field and value can therefore identify a specific action being taken by a patient.</p> <p>For example, ea=Clicked Request/Book Appointment/Online Button</p>
el	<p>Value = Event Label</p> <p>Explanation: The “el” field equals a value that provides further specificity as to the “event” (e.g. action) being taken by a patient. According to Google, this field “[s]pecifies the event label.”¹⁹ The “el” field and value can therefore identify a specific action being taken by a patient.</p> <p>For example, el=user_action.alter_view.request_appointment</p>
dl	<p>Value: Full URL</p> <p>Explanation: The “dl” (document location) field is equal to a value that identifies the full URL of the webpage that a patient is viewing. Google acknowledges that the “dl” field and value is “content information.”²⁰ The “dl” field and value therefore identifies and transmits the content of the patient’s current communication.</p> <p>For example, dl= https://providers.gundersenhealth.org/provider/Jason+R.+Darrah/2067523?alias_term=Cardiology&specialty strict=Cardiology.*&sort=relevance%2Cnetworks%2CAv</p>

¹⁶ See Ex. 7, *How Google Analytics Collects Data*, ANALYTICS MARKET, at 2, <https://www.analyticsmarket.com/blog/how-google-analytics-collects-data/>; Ex. 8, *Measurement Protocol Parameter Reference*, GOOGLE FOR DEVELOPERS/ANALYTICS, at 7, <https://developers.google.com/analytics/devguides/collection/protocol/v1/parametersparameters>.

¹⁷ *Id.* (Ex. 8) at 10.

¹⁸ *Id.* (Ex. 8) at 10-11.

¹⁹ *Id.* (Ex. 8) at 11.

²⁰ *Id.* (Ex. 8) at 8.

Field	Value and Explanation
	availability_density_best&from=search-list
dt	<p>Value: The title of the page or document that is being viewed</p> <p>Explanation: The “dt” field (document title) equals a value that identifies the document title of the web page being viewed. Google acknowledges that the “dt” field and its value is “content information.”²¹ The “dt” field and value identifies and transmits the content of a patient’s specific communication.</p> <p>For example, with respect to the above “dl” example, the accompanying dt field (sent in the same query string parameter) = Dr. Jason R. Darrah,–MD - La Crosse,–WI - Cardiology - Book Appointment</p>
jid	<p>Value: Allows Syncing of Information between Google Analytics, Google Ads, and Google Display Ads</p> <p>Explanation: The “jid” field equals a numeric value that is an identifier and a Join ID. This value enables Google to match patient information that Google Analytics has obtained with information obtained through the domain Doubleclick.net (Google Display Ads).²² Upon information and belief, it also allows Google to match patient information that Google Analytics has obtained with information obtained through the domain www.Google.com (Google Ads).</p>
gjid	<p>Value: Allows Syncing of Information between Google Analytics and Google Display Ads</p> <p>Explanation: The “gjid” field equals a numeric value that is an identifier and Join ID. This value enables Google to match patient information that Google Analytics has obtained with information obtained through the domains Doubleclick.net (Google Display Ads).²³</p>
cid	<p>Value: Unique Patient Identifier</p> <p>Explanation: According to Google, “[t]his field … identifies a particular user, device, or browser instance. For the web, this is generally stored as a first-party cookie with a two-year expiration. For mobile apps, this is randomly generated for each particular instance of an application install. The value of this field should be a random UUID (version 4) as described in http://www.ietf.org/rfc/rfc4122.txt.²⁴ The corresponding value is a unique alphanumeric identifier and it contains the _ga cookie value that is disguised as a “first-party” cookie by Google.</p>
tid	Value: Identifier for the Health Care Provider

²¹ *Id.* (Ex. 8) at 9-10.

²² Ex. 7, *supra* n.16 at 2 (explaining that the “jid” field provides the “Join ID for DoubleClick beacon”).

²³ *Id.* (Ex. 7) at 2 (explaining that the gjid is the “tracking code version” of the “gid”).

²⁴ Ex. 8, *supra* n.16 at 5.

Field	Value and Explanation
	Explanation: Google explains that the “tid” equals an alphanumeric value that is a “tracking ID/web property ID. The format [of the value] is UA-XXXX-Y. All collected data is associated by this ID.” ²⁵
_gid	Value: Potential Unique Patient Identifier
	Explanation: The field equals a numeric value that is a unique patient identifier because it is a user ID that can be used to distinguish users. ²⁶
Gtm	Value: Identifier for the Health Care Provider
	Explanation: This field equals an alphanumeric value that corresponds to the advertiser’s Google Tag Manager account. ²⁷ It can therefore potentially identify the patient’s Health Care Provider (e.g. where the proposed targeted advertisement may appear).

67. Google disseminates Google Source Code to obtain data for Google Analytics in numerous ways. One of the Google products and services through which Google Analytics captures Health Information, the Google Analytics Measurement Protocol, is discussed in more detail below.

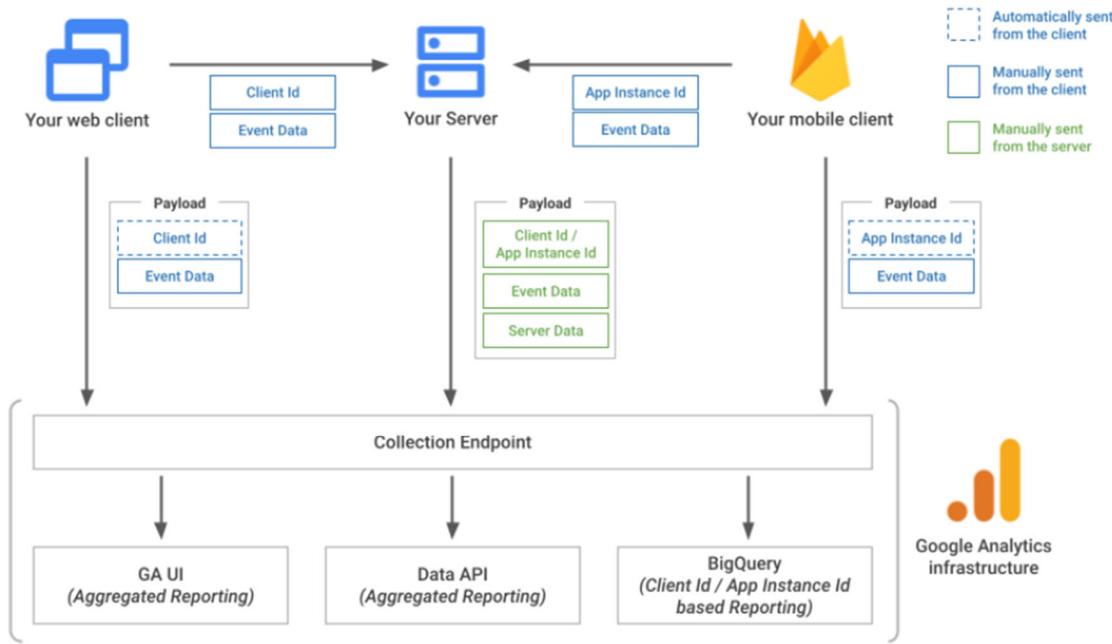
///
///
///
///
///
///
///
///
///
///
///
///
///
///
///

²⁵ *Id.* Ex. 8 at 1.

²⁶ Ex. 7, *supra* n.16 at 2 at 2.

²⁷ Ex. 9, *Set Up and Install Tag Manager*, GOOGLE TAG MANAGER HELP, at 2, <https://support.google.com/tagmanager/answer/6103696>. “GTM” is an abbreviation for Google Tag Manager.

68. **Google Analytics Measurement Protocol.** The Google Analytics Measurement Protocol (GMP) is an aspect of the Google Source Code associated with Google Analytics. Google has published the following “Architectural Overview” depicting how data is sent, either from web-based users or app-based users, through GMP to Google Analytics.



As illustrated in the above diagram, regardless of the means, Google intercepts from both web-based and app-based users (at a minimum) the Client ID or App Instance ID (both used to uniquely identify the user) and event data (described further below).

69. All GMP products integrate with “Floodlight,” another version of Google’s Source Code that, similar to Google Tag and the Firebase SDK (both discussed further below), track activity across a specific web property or mobile application.

70. One of the most popular means for Google to retrieve data via GMP is through what is known as a “POST” or “GET” request. Both requests require an HTTP request to “<https://google-analytics.com/collect>” or one of Google’s other domains.

71. Google recommends that website owners use the POST request because it enables a “larger payload” i.e., it intercepts more data and, when POST requests are not available, to send data via the GET requests. In either case, Google receives through these requests at least the following data in Google’s preferred code so that it can interpret the data, as well as the URL of the website the user visited, as illustrated by Google’s description in the figure below of “required values” for payload data:²⁸

The following parameters must be in each payload:			
Name	Parameter	Example	Description
Protocol Version	v	v=1	The protocol version. The value should be 1.
Tracking ID	tid	tid=UA-123456-1	The ID that distinguishes to which Google Analytics property to send data.
Client ID	cid	cid=xxxxx	An ID unique to a particular user.
Hit Type	t	t=pageview	The type of interaction collected for a particular user.

b. Google Ads

72. Google Ads is Google’s advertising system for Google’s eponymous search engine at www.Google.com, which Google markets as a way to “create online ads to reach people exactly when they’re interested in the products and services that you offer.”

73. Google Ads works by collecting information, via the Google Source Code, about user searches directly at www.Google.com and their communications on advertiser or publisher web properties outside of Google-owned domains, including Health Care Providers’ web properties (e.g. www.gundersenhealth.org and www.medstarhealth.org), where the Google Source

²⁸ Ex. 10, *Measurement Protocol Reference*, GOOGLE FOR DEVELOPERS/ANALYTICS, at 3, <https://developers.google.com/analytics/devguides/collection/protocol/v1/reference>.

Code for Google Ads is present. For example, when a patient exchanges a communication with their Health Care Provider about a specific doctor, condition, or treatment, the content of that communication will be intercepted by Google Ads and sent to google.com, even though the patient took no action on google.com.

74. Google Ads is associated with the following domains and subdomains:

- a. www.google.com/pagead/1p-user-list²⁹;
- b. www.google.com/maps;
- c. www.google.com/ads/ga-audiences;
- d. adservice.google.com;
- e. www.google.com/ads/measurement;
- f. fcmatch.google.com;
- g. ade.googlesyndication.com;
- h. pagead2.googlesyndication.com;
- i. tpc.googlesyndication.com; and
- j. www.googleadservices.com.

75. Upon information and belief, based on the investigation of counsel and expert analysis, Google Source Code redirects patient Health Information to Google Ads on approximately 59 percent of Health Care Provider properties analyzed by Plaintiffs' expert.

76. When the Google Source Code for Google Ads is present on a patient's Health Care Provider's web property, the Google Source Code tracks, intercepts and collects the patient's Health Information.

77. Cookies: When the Google Source Code for Google Ads is present on a Health Care Provider's web property, the source code deposits an NID Cookie (or accesses an existing NID Cookie) on the patient's computing device. The NID cookie contains a device identifier that

²⁹ These URLs represent the endpoints of servers through which Google acquires information about Internet communications. They are not meant to be viewed by actual users. Thus, typing these URLs into a browser toolbar will not render any readable content.

is associated with Google's Search engine, www.Google.com. That same NID cookie is also deposited when a patient interacts (either before or after their visit with their Health Care Provider's web property) with www.Google.com (i.e. Google Ads). Thus, the NID Cookie is lodged on both Google and non-Google web properties. By redirecting this identifier to Google.com when a patient is on a non-Google website and transmitting it when a patient is directly on Google.com, Google is able to use the patient's activity on non-Google websites relating to health (such as on Gundersen's web property) for purposes of behaviorally targeted advertising based on those health communications that occur on Google's eponymous search engine. Similarly, if a patient has a Google Account, and is signed-in to that account while browsing, the Google Source Code will track any Internet communications with a Google Account ID that is a unique identifier specifically connected to her Google Account – sending that information to Google.com when the patient is on a non-Google healthcare web property for the same types of usage. In this situation, the Google Source Code will send both the NID cookie and the Google Account ID to Google, creating an association between the two such that any future communication by a patient who is not signed into her Google Account can be identified by Google by using the NID cookie to link that patient to her Google Account ID.

78. Identifiers: When the Google Source Code for Google Ads is present on a Health Care Provider's web property, the source code causes the redirection of patient identifiers to Google.

79. For example, when a patient interacts with MedStar's web property, including its patient portal, the Google cookies and identifiers that the Google Source Code causes to be redirected to Google Ads may include and are not limited to:

- a. The patient's IP address;
- b. The patient's User-Agent;
- c. Google Analytics cookies that are disguised as first-party cookies, i.e.,
_ga, _gid, and _gcl_au;

- d. Google Ads cookies, including cookies directly associated with a patient's Google Account (if they have one) and cookies directly associated with a patient's computing device (named NID cookies);
- e. Patient device identifiers; and
- f. Patient device attributes sufficient to uniquely identify the device under "entropy".

80. Request URL: When the Google Source Code for Google Ads is present on a Health Care Provider's web property, the source code causes the redirection of Request URLs to Google, including file-path information that includes information relating to the substance, purport, or meaning of the communications patients exchange with their Health Care Provider.

81. For example, when patients interact with MedStar's web property, including its patient portal, the information about the substance, purport, and meaning of the patients' communications with their Health Care Provider that is intercepted by the Google Source Code and redirected to Google Ads may include and is not limited to:

- a. The Request URL, and portions thereof that specifically identify doctors, conditions, treatments, services, prescription drugs, payment information, health insurance information, appointment requests, and log-in/log-out information that were the subject of communications exchanged between patients and their Health Care Providers; and
- b. Join IDs that enable Google to join identifiers and communications content collected through Google Analytics with identifiers and communications content collected through Google Ads.³⁰

³⁰ Upon information and belief, a Join ID is a unique value that can be shared across products (e.g. shared between Google Analytics, Google Ads and Google Display Ads) and then used by a company (e.g. Google) to cross-reference and join that information together, across products.

82. Examples of Request URLs and portions thereof that are intercepted by the Google Source Code and re-directed to Google Ads from MedStar's web property (alongside patient identifiers) may include and are not limited to:

- a. Searches for a doctor on MedStar's web property;
- b. Requests for an appointment on MedStar's web property;
- c. Search terms, results, or other communications relating to MedStar health services, conditions, tests, and treatments, for example:

<https://www.medstarhealth.org/services/abdominal-aneurysm-treatment;>

<https://www.medstarhealth.org/services/blood-cancer-treatments;> and

<https://www.medstarhealth.org/services/behavioral-health-treatments;>

- d. Patient communications to log-in to or enroll in the MedStar patient portal;
- e. Information about communications exchanged by patients after they have logged-in to the MedStar patient portal; and
- f. Patient communications to log-out of the MedStar patient portal.

83. Query String Parameters: Examples of Query String Parameters intercepted by the Google Source Code and redirected to Google Ads include the above tid, cid, and jid fields, as well as:

FIELD	VALUE AND EXPLANATION
Eid	<p>Value: Potential Unique Identifier</p> <p>Explanation: Upon information and belief, the "eid" field equals a numerical value that is a potential unique identifier. Plaintiffs reasonably believe 'eid' is an "Event ID" that can be used to track a specific, unique event across Google Display Ads (i.e. Doubleclick.net) and Google Ads (i.e. google.com) for events that Google tracks on non-Google properties. The same 'eid' value is re-directed to DoubleClick.com (Google Display Ads) and Google.com (Google Ads) for the same events that Google tracks on a Health Care Provider's web property, e.g. www.gundersenhealth.org.</p>
URL	<p>Value: Full URL Location</p> <p>Explanation: Upon information and belief, the URL field equals the full</p>

FIELD	VALUE AND EXPLANATION
	URL of the page that an individual is viewing. For example, URL = https://www.gundersenhealth.org/patients-visitors/mychart/ .
Tiba	<p>Value: Document Title</p> <p>Explanation: Upon information and belief, the “tiba” field equals the title of the page or document that is being viewed by the patient.</p> <p>For example, document title for the above URL example is tiba= What can I do with MyCha-t? - Gundersen Health System.</p>
NID	<p>Value: Unique Patient Identifier</p> <p>Explanation: Upon information and belief, the NID field is a Google cookie that contains a unique alphanumeric value that is associated with and redirected to Google.com (Google Ads). The alphanumeric value uniquely identifies the specific browser on the patient’s specific device.</p>
Secure-3PSID Secure-3PAPISID Secure-3PSIDCC	<p>Value: Unique Patient Identifier linked to a Google Account</p> <p>Explanation: Upon information and belief, these fields equal a unique alphanumeric value, which is logged when a Google Account Holder is signed into their account and is associated with a patient’s Google Account.</p>

c. Google Display Ads

84. Google Display Ads is Google’s advertising system for its Display Ads network.

85. Google Display Ads works by collecting information about user communications on non-Google websites, e.g., a Health Care Provider web property, for use in serving targeted ads to users when they are on non-Google websites based on remarketing, targeting by user characteristics and interests (including the content of pages where the ads would appear).

86. Google Display Ads is associated with the following domains, sub-folders, and sub-domains:

- a. www.doubleclick.net;
- b. googleleads.g.doubleclick.net;
- c. stats.g.doubleclick.net;
- d. securepubads.g.doubleclick.net;

- e. bid.g.doubleclick.net; and
- f. cm.g.doubleclick.net.

87. Upon information and belief, based on investigation of counsel and expert analysis, Google Source Code redirects patient Health Information to Google Display Ads on approximately 50 percent of Health Care Provider web properties analyzed by Plaintiffs' expert.

88. When the Google Source Code for Google Display Ads is present on a patient's Health Care Provider's web property, the source code tracks, intercepts and re-redirects patient Health Information to Google Display Ads.

89. Cookies: When the Google Source Code for Google Display Ads is present on a Health Care Provider's web property, the source code deposits the DSID and IDE Cookies onto the patient's computing device. The DSID cookie is associated with a Google Display Ad (e.g., www.DoubleClick.net), and contains a value that can identify a patient's Google Account (if they have one). The IDE cookie is also associated with a Google Display Ad (e.g. www.DoubleClick.net), and it contains a value that can identify the patient's device – the specific browser instance.³¹ Thus, the DSID and IDE cookies can be used to uniquely identify and track individuals as they navigate the Internet, including as they communicate with their Health Care Providers' web properties. Similar to Google Ads, Google associates the DSID and IDE cookies for specific patients and their devices to each other by acquiring them at the same time when a person is logged-in to their Google Account. Thereafter, Google's acquisition of either cookie by itself is sufficient for Google to associate any event acquired with the other cookie.³²

³¹ A browser “instance” refers to a specific browser on a specific device. For example, John Doe may have Chrome on a desktop computer. Google assigns John Doe’s Chrome application on that specific computer an identifier that is unique to John Doe, that device, and that browser on the device. Google separately tracks app instances, i.e., a specific app on a specific device, with the Instance ID.

³² To give a non-technology example of how this works: imagine reviewing a basketball program that contains the players’ names and numbers, upon learning that No. 30 for the Golden State Warriors is Steph Curry, any subsequent information you receive about No. 30 can easily be correlated with Steph Curry. Likewise, any information you receive about Steph Curry can easily be correlated with No. 30 for the Golden State Warriors.

90. Identifiers: When the Google Source Code for Google Display Ads is present on a Health Care Provider's web property, the source code redirects identifiers to Google.

91. For example, when a patient interacts with MedStar's web property, including its patient portal, the Google Cookies and identifiers that the Google Source Code causes to be redirected to the Google Display Ads may include and are not limited to:

- a. The patient's IP address;
- b. The patient's User-Agent;
- c. Google Analytics cookies that are disguised as first-party cookies, i.e., _ga, _gid, and _gcl_au;
- d. Google Display Ads cookies, including cookies directly associated with a patient's Google Account (named DSID, if they have a Google Account) and cookies directly associated with a patient's computing device (named IDE cookies);
- e. Patient device identifiers; and
- f. Patient device attributes sufficient to uniquely identify the device under "entropy".

92. Request URL: When the Google Source Code for Google Display Ads is present on a Health Care Provider's web property, the source code redirects Request URLs to Google. For example, when a patient interacts with MedStar's web property, including its patient portal, the information about the substance, purport, and meaning of patient communications with the Health Care Provider that is intercepted by the Google Source Code and redirected to Google Display Ads may include and is not limited to:

- a. The Request URL, and portions thereof that specifically identifies doctors, conditions, treatments, services, prescription drugs, payment information, health insurance information, appointment requests, and log-in/log-out information that were the subject of communications exchanged between a patient and their Health Care Providers; and

b. Join IDs that enable Google to join identifiers and communications content collected through Google Analytics with identifiers and communications content collected through Google Ads.

93. Examples of Request URLs and portions thereof that are intercepted by the Google Source Code and redirected to Google Display Ads from the MedStar web property (alongside patient identifiers) may include and are not limited to:

- a. Searches for a doctor on MedStar's web property;
- b. Requests for an appointment on MedStar's web property;
- c. Search terms, results, or other communications relating to MedStar's services, conditions, tests, and treatments, for example:

<https://www.medstarhealth.org/services/abdominal-aneurysm-treatment;>

<https://www.medstarhealth.org/services/blood-cancer-treatments>; and

<https://www.medstarhealth.org/services/behavioral-health-treatments>;

- d. Patient communications to log-in to or enroll in the MedStar patient portal;
- e. Information about every communication exchanged by patients after they have logged-in to the MedStar patient portal; and,
- f. Patient communications to log-out of the MedStar patient portal.

94. Query String Parameters: When the Google Source Code for Google Display Ads is present on a Health Care Provider's web property, the source code redirects Query String Parameters to Google. Examples of Query String Parameters intercepted by the Google Source Code and redirected to Google Display Ads may include and are not limited to: the tid, cid, jid, gjid, _gid, eid, URL, tiba fields and values (described above), as well as:

FIELD	VALUE AND EXPLANATION
	Value: Potential Unique Identifier
aud	Explanation: Upon information and belief, this field is equal to a value that is identical to the _gcl_au cookie (which Google disguises as a first-party cookie on MedStar's web property), and overlaps substantially with the _ga cookie that Google also disguises as a first-party cookie on Health Care Providers' web properties, e.g. the

FIELD	VALUE AND EXPLANATION
	Gundersen web property. Upon information and belief, this identifier ties a patient's identifiers together for Google across Google Analytics and Google Display Ads.
IDE	<p>Value: Unique Patient Identifier</p> <p>Explanation: As explained above, the IDE field equals an alphanumeric value that is the same as the IDE cookie (which is a Google cookie that re-directs to www.Doubleclick.net). The IDE cookie value allows tracking of a user for advertising purposes by Google. Upon information and belief, by transmitting the IDE field together with the auid cookie, Google is effectively linking these identifiers to cross-identify patient's browsing histories.</p>
DSID	<p>Value: Unique Patient Identifier</p> <p>Explanation: As explained above, the DSID field equals an alphanumeric value that is the same as the DSID cookie (which is a Google cookie that re-directs to www.Doubleclick.net). Upon information and belief, the DSID cookie value allows tracking of a user for advertising purposes by Google.</p>

d. **Google Tag and Tag Manager, Firebase SDK, Google APIs and YouTube**

95. In addition to the above, Google Tag and Tag Manager, Google Firebase SDK, Google APIs, and YouTube (including YouTube TV) are additional Google products and services which operate on web properties through the use of Google Source Code.

96. **Google Tag** (gtag.js) is a small piece of JavaScript code that can be incorporated on a web property, streamlining the placement of multiple Google product source codes into a single “tag.” Google explains: “The Google tag (gtag.js) is a single tag you can add to your website to use a variety of Google products and services (e.g., Google Ads, Google Analytics, Campaign Manager, Display & Video 360, Search Ads 360). Instead of managing multiple tags for different Google product accounts, you can use the Google tag across your entire website and connect the tag to multiple destinations.”³³ Google Tag includes a piece of code called a “trigger” which is “fired” or activated whenever it detects that a user has performed certain “events” (i.e., actions and

³³ Ex. 11, *About the Google Tag*, GOOGLE FOR DEVELOPERS/TAG PLATFORM, at 1, <https://developers.google.com/tag-platform/gtagjs>.

communications) on a website.³⁴ Google markets the ease of incorporating Google Tag on web properties, encouraging web developers to merely “[c]opy and paste” its code into their existing web pages.³⁵

97. **Google Tag Manager** is a source code that Google offers to web-developers to streamline management of source code that is placed on their properties. Whereas Google Tag is designed to incorporate Google products, Google Tag Manager can be used to incorporate both Google and non-Google (“third-party”) products and services, such as tracking code deployed by other entities.³⁶ Streamlining multiple parties’ source code in this way, by combining it within Google Tag Manager, facilitates the rapid transmission of data to Google by eliminating or reducing delays inherent in loading code from multiple sources. In addition to streamlining source code, Google Tag Manager also intercepts information transmitted between an individual and the web property, including Health Care Provider web properties, with which they are communicating.

98. After acquiring the contents of communications exchanged between patients and their Health Care Providers, Google re-directs those contents and patient identifiers to the entities whose source code is incorporated in the Google Tag Manager. Entities who receive the contents and identifiers within online communications from Google in this way include other companies engaged in Internet surveillance, such as Twitter, Microsoft, and Pinterest.³⁷

99. The re-directions from the Google Tag Manager source code to other ad tech companies occurs in a two-step process. *First*, Google Tag Manager source code on the Health Care Provider web-properties commands the patient’s communications device to re-direct the content of the communication with their Health Care Provider to Google at

³⁴ “Events” are also available in Google’s SDKs, described further below.

³⁵ Ex. 9, *supra* n.27 at 3.

³⁶ Ex. 12, *Tag Manager and the Google Tag*, GOOGLE TAG MANAGER HELP, at 3, <https://support.google.com/tagmanager/answer/7582054>.

³⁷ Google Tag Manager provides “native” sharing for 79 companies and at least 879 others in its “templates” section. *See* <https://support.google.com/tagmanager/answer/6106924>? (listing “native”) and <https://tagmanager.google.com/gallery/#/?page=1> (others).

www.googletagmanager.com. *Second*, Google Source Code at www.googletagmanager.com will then command the patient’s communications device to further re-direct the content and patient identifiers to the third party. The patient identifiers sent to those other ad tech companies will include IP address + User-Agent, and device identifiers such as persistent cookies that the other ad tech companies use for surveillance. In many cases, the Google Tag Manager will facilitate a process called “cookie matching” between Google and the other ad tech companies or between the various ad tech companies with one another. In this process, Google and the other ad tech companies help ensure that each other can deterministically or probabilistically identify the patient and/or their household.

100. This re-direction of the patient identifiers and communications content to other ad tech companies occurs from source code present directly on Google’s servers for www.googletagmanager.com.

101. All steps of the process occur in the background while the underlying communication between the patient and the Health Care Provider are still ongoing.

102. **Google Firebase SDK**³⁸ is pre-packaged source code created by Google for mobile applications. Google designed its SDKs, including Firebase, to transmit data from the mobile app user’s device to Google’s servers (known as the endpoints).³⁹ In addition to event data, the Firebase SDK also intercepts user identifiers. For instance, the Firebase SDK intercepts an “app-instance identifier” which is used to track a unique installation of the app. So long as the app remains installed, using the app-instance identifier Google can uniquely identify the user, as well as their interactions and events, using this ID. The Firebase SDK also intercepts the Android Advertising ID, from Android devices, and Apple’s Identifier for Advertisers (“IDFA”), from iOS devices, which are device-specific identifiers.

³⁸ Google Firebase SDK is now known as “GA4F” or “Google Analytics for Firebase.”

³⁹ The Firebase SDK was launched in 2018. Google previously offered another SDK called the Fabric SDK, which operated in a manner similar to the Firebase SDK. The Fabric SDK was deprecated in November 2020.

103. **Google APIs** is a service that Google offers to integrate information on web properties. In addition to these integration services, Google APIs source code also intercepts information transmitted between an individual and the web property, including Health Care Provider web properties, with which they are communicating.

104. **YouTube** is Google's video viewing service at www.YouTube.com, and YouTube TV is Google's streaming cable service at TV.YouTubeTV.com (together, "YouTube"). In addition to these video services, YouTube source code also intercepts information transmitted between an individual and the web property, including Health Care Provider web properties, with which they are communicating. Cookies that are associated with YouTube include, but may not be limited to "YEC" and "Visitor_Info1_Live".

105. Each of the above products and services transmit persistent unique identifiers for the users of web properties and "event" data regarding their interactions and communications with Healthcare Providers to Google, which Google uses for its marketing and advertising purposes including, on information and belief, for segmenting and categorizing individuals within the "health vertical" classification system described in Section IV-F, below.

2. Google's Offline Acquisition of Health Information

106. In addition to unlawfully acquiring Health Information via the Google Source Code, Google's interception of Health Information also occurs from "offline" sources.

107. For example, in conjunction with its advertising systems, Google offers a program called Customer Match.

108. As described by Google, "Customer Match lets [advertisers] use [their] online and offline data to reach and re-engage with [their] customers across [Google] Search, the Shopping tab, Gmail, YouTube, and Display. Using information that [advertisers'] customers have shared with [them], Customer Match will target ads to those customers and other customers like them."⁴⁰

⁴⁰ Ex. 13, *About Customer Match*, GOOGLE ADS HELP, at 1, <https://support.google.com/googleads/answer/6379332>.

109. Google provides the following explanation as to how Customer Match works:⁴¹

How it works		
Let's say you want to advertise a new loyalty program to your existing customers with Google ads. Here's how it works:		
1 You create and upload a <i>customer list</i> data file of contact information your customers have given you. Use this template and check this article for formatting instructions.	2 You create or update a campaign to target your Customer Match segment – customers from your uploaded data file who are Google users.	3 When those users are signed in to their Google account, they come across your ads when they use the Search Network, YouTube, and Gmail or when they browse on the Google Display Network.

110. In other words, Google's Customer Match program allows its advertisers, like Health Care Providers, to match their audiences', e.g., patients', online and offline information – including matching online and offline patient Health Information.

111. As indicated in the Table above, the offline Health Information is uploaded and provided to Google.

112. The matching is done by Google. Google explains that once it is in possession of the offline data, it matches that offline data to existing Google Accounts, and will use the Customer Match data to create Customer Match Audiences, i.e., a Customer Match list for purposes of targeted advertising through Google's advertising systems.⁴²

113. This is all done for the purpose of targeted advertising through Google's advertising systems.⁴³

⁴¹ *Id.* (Ex. 13) at 3.

⁴² Ex. 14, *How Google Uses Customer Match Data*, GOOGLE ADS HELP, <https://support.google.com/google-ads/answer/6334160> ("The customer data files you upload will only be used to match your customers to Google accounts[.]") (underlined in original indicating hyperlink). Google's explanation of *How Google Uses Customer Match Data* contains many references to Google's commitment to privacy and adherence to its own policies, but the very purpose of Customer Match is for Google to connect online and offline information for the purposes of digital advertising through its own advertising systems.

⁴³ Ex. 15, *Create a Customer List*, GOOGLE ADS HELP, at 1, <https://support.google.com/google-ads/answer/6276125> (explaining that Customer Match "lets you target ads to your customers using the data they share with you.").

114. Google is, therefore, not only unlawfully acquiring Health Information via the Google Source Code, but also unlawfully acquiring it via offline resources.

C. Google Is Not Just a “Vendor”

115. Google is not a mere vendor to Health Care Properties.

116. As alleged throughout this complaint, Google uses the data that it acquires from Health Care Provider web properties for itself, including to monetize it, and also shares the information with dozens of other companies without patient authorization.

117. Even when Google does not directly monetize the Health Information, it uses it to learn aggregate information to improve Google’s own business – not the business of those publishers or advertisers on whose properties Google is collecting data. Among other things, Google uses the information collected to:

- a. Improve its search algorithms and other ad-related capabilities, including ad targeting and attribution;
- b. Improve its machine learning models;
- c. Conduct experiments for its own business purposes;
- d. Aggregate the data for business analysis purposes; and
- e. Encourage and induce a free Analytics customer to become a paying customer of Google Ads, Google Display Ads, YouTube, and its other tools.

118. Google’s collection techniques also enable it to provide detailed reports on all activity that occurs on a web-property, which amounts to data mining. While Google may provide reports to Health Care Providers showing aggregate or anonymized statistics, Google maintains access to real identifiers and the identity of those users in its own databases for its own purposes.

119. Google’s collection of information on specific Health Care Properties is not limited to small acquisitions of discrete information but instead involves surveillance of a Health Care Provider’s entire or nearly entire web-property, including all pages relating specifically to doctors, conditions, treatments, symptoms, appointments, and patient portals.

120. Google expressly recommends to publishers that its “tag should be installed on every page of your website” and, as a result, more frequently than not, Google acquires Health Information from every page on a Health Care Provider’s web-property.⁴⁴

121. Google also recommends that publishers place its source code early on every webpage, such as in the header, to ensure that Google has access to all communications exchanged on a web-property from which it is acquiring data through the Google Source Code.

122. Google is, therefore, not only unlawfully acquiring Health Information via the Google Source Code, but also unlawfully acquiring it via offline resources.

D. How Google Monetizes the Health Information

123. After tracking, intercepting and acquiring patients’ Health Information, Google uses the information for personalized advertising in its advertising systems which includes, but is not limited to, Google Analytics, Google Ads, and Google Display Ads.

124. Because Google Analytics, Google Ads, and Google Display Ads and the other products and services discussed in Section IV-B above are advertising products, Google’s acquisition of Health Information through, and use of Health Information within, the products constitutes advertising use of Health Information, regardless of whether it is later used to serve an advertisement to a patient or not.

125. For example, two features of Google Ads through which Google monetizes Health Information, and which are particularly profitable to Google, are its Audience Targeting and Conversion Tracking capabilities.

126. Audience Targeting refers to serving ads to only a select number of users who share certain common characteristics. For Google’s Audience Targeting, Google can target ads to either “Pre-defined Google Audiences” or “Advertiser-curated Audiences.” Pre-defined Audiences are those created by Google based on interest and demographic data. Advertiser-curated Audiences

⁴⁴ Ex. 16, *Use the Google Tag for Google Ads Conversion Tracking*, GOOGLE ADS HELP, at 1, <https://support.google.com/google-ads/answer/7548399>.

are customized audiences created by Google through the use of the Source Code, including audiences created through Google Analytics, either (1) by directly intercepting data using Google Tag, SDKs, or other Google Source Code with a destination set to Google Ads; or (2) via linking of a Healthcare Provider's Google Ads account to their Google Analytics account, if they have one, and uploading of their Google Analytics audiences to Google Ads.

127. Conversion Tracking refers to Google Ads' feature that tracks whether a user has engaged in activity or communicated on a website or app (e.g., purchasing a product or clicking a specific link). Conversion Tracking can be added to a specific website or app (rather than just a singular ad) by incorporating Google's Source Code. The Source Code places a temporary cookie on the user's desktop or mobile device when they click an ad or ad video, and once the desired action is taken, recognizes the cookie and records a conversion.

128. The Conversion Tracking feature can utilize Health Information and, among other things, enable Target CPA bidding (target cost-per-action) which is an automated bidding strategy that sets bids to get as many conversions as possible. Target CPA accomplishes the automatic bidding for its client by evaluating the "contextual signals," which include the remarketing list (audience created for advertising) that the user belongs to, the user's search query that triggered that ad, the user's behavior on the website or app, and various other user attributes.

129. Additionally, the data collected from Google's Source Code powers Google Ads' attribution models which assess the effectiveness of ads and specifically, evaluates how much credit each ad interaction deserves for a successful conversion. The attribution models are used to determine whether Google paid channels or other channels are responsible for a conversion. This feature is essential to Google's advertising business because it demonstrates the efficiency of Google's services.

130. In addition to the above, Google internally utilizes Health Information for Remarketing on Google owned-and-operated web properties, and for targeted advertising on non-Google owned-and-operated web properties.

1. Google's Monetization of Health Information for Remarketing Across Google's Marketing Channels

131. Remarketing (also referred to as retargeting) is the practice of targeting specific ads to people based on actions they have taken on an advertiser's website.

132. Positive remarketing occurs when Google targets patients based on specific actions or communications exchanged online or offline with a Health Care Provider. For example, a positive retargeting campaign may target ads about cancer treatment to people who: (1) have logged-in to their patient portal; and (2) exchanged communications with the hospital about cancer. This subsequent ad, based on prior actions and communications, is remarketing or retargeting.

133. Negative remarketing occurs when Google decides not to target advertisements to specific persons based on their actions or communications exchanged online or offline with a Health Care Provider, typically because that person has already purchased a particular product. For example, a negative retargeting campaign may decide that an ad seeking new patients should not be shown to anyone who has previously logged-in to a Health Care Provider's patient portal or communicated about a specific subject matter. In this example, Google would identify patients who fit that description as they use Google.com or other web properties and avoid showing the patient acquisition ads from their Health Care Provider.

134. Google uses Health Information for purposes of remarketing on Google Search, www.Google.com.

135. For example, when, at any point after visiting their Health Care Provider's web property, the patient later visits www.Google.com to conduct a search, Google uses the previously intercepted Health Information to influence the patient's search results through targeted remarketing or retargeting campaigns.

136. Specifically, Google Ads has a program called Remarketing Lists for Search Ads (RLSA), which enables advertisers to "customize" Search Ads campaigns "for people who have

previously visited [the advertisers'] site, and tailor ... bids and ads to these visitors when they're searching on Google and search partner sites.”⁴⁵

137. Google explains how it works:⁴⁶

How it works

You can create audience segments to target with your Search ads that include people who have left your website without buying anything. Your Search ads will then help you connect with these potential customers when they continue looking for what they need using Google Search. Set your bids, create ads, or select keywords keeping in mind that these potential customers have previously visited your website.

There are two basic strategies for using your data segments with Search ads:

- You can optimize bids for your existing keywords for your website visitors and app users. For example, you can increase your bid by 25% for those who previously visited your website in the last 30 days. Or, you could show a different ad to site visitors who have placed items in a shopping cart but have not purchased them.
- You can bid on keywords that you don't normally bid on just for people who have recently visited your site, or have converted on your site in the past. This can help you increase your sales. For example, you could bid on more broad keywords only for people who have previously purchased from your site.

Keep in mind: The membership limit for these lists is capped at 540 days. [Learn more About your data segments.](#)

138. Google then provides an example:

Example

People looking for running shoes visit a sports apparel website to check out the available styles, and look at the shoe section of the site. The site could add these shoppers to a "Shoe category" list. Then, for example, the site could bid more for these visitors next time they search for running shoes on Google.

139. On a page titled “About your data segments,” Google explains to advertisers how they can use their “data to re-engage people who have previously interacted” with their “brand or

⁴⁵ Ex. 17, *About Your Data Segments for Search Ads*, GOOGLE ADS HELP, at 1, <https://support.google.com/google-ads/answer/2701222>.

⁴⁶ *Id.* (Ex. 17) at 1-2.

services on mobile or desktop” so that their “ads are shown to people in this segment as they browse Google or partner websites.”⁴⁷

140. Google explains how advertisers can “Tag your website using Google Ads.”⁴⁸ This page explains that doing so “helps [the advertiser] reach people who have visited [their] website or who have used [their] app.” Google also explains that “[t]he Google tag is a web tagging library for Google’s site measurement, conversion tracking, and products using your data segments. It’s a block of code that adds your website visitors to your data segments, allowing you to target your ads to these visitors. For dynamic remarketing, you’ll also use event snippets, which passes specific data to Google Ads about your website visitor and the actions that they take on your site.”

141. Google allows Health Care Providers to engage in Remarketing Lists for Search Ads and, in such cases, rather than bidding more for people searching for running shoes on Google, the Health Care Providers are encouraged to bid more for patients. For example, a Health Care Provider may increase the amount it is willing to pay to appear in the ad results for a Google Search based on the fact that the user is a patient or has exchanged a certain type of communication with the Health Care Provider, e.g., asking about cancer.

142. Google also enables Health Care Providers to engage in the “negative remarketing” outlined above.⁴⁹ For example, if a hospital were running an advertising campaign to convert existing patients into purchasers of specific additional health care services, the hospital would engage in a positive remarketing campaign towards known patients who exchanged communications about specific topics. However, if a hospital were running an advertising

⁴⁷ Ex. 18, *About Your Data Segments*, *your data segments*, GOOGLE ADS HELP, at 1, <https://support.google.com/google-ads/answer/2453998>.

⁴⁸ Ex. 19, *Tag Your Website Using Google Ads*, GOOGLE ADS HELP, at 1, <https://support.google.com/google-ads/answer/2476688>.

⁴⁹ Ex. 20, *Prevent Ads from Displaying to Members of Google Ads Remarketing Lists: Create a Negative Remarketing Target*, SEARCH ADS 360 HELP, at 1, <https://support.google.com/searchads/answer/6108309>.

campaign to obtain new patients, it may choose to engage in negative remarketing or retargeting by telling Google to identify and exclude existing patients from that advertising campaign.

143. In addition to using Health Information to enable Health Care Providers to engage in remarketing at www.Google.com (Google Ads), Google also uses Health Information to enable remarketing on Google Analytics, Google Display Ad Network and YouTube.⁵⁰

144. For example, if a pharmaceutical company wants to target ads to patients who have previously exchanged communications about the company's prescription drugs, it may create a remarketing campaign on that topic that runs across Google Ads, Google Analytics, Google Display Ads, and YouTube.

145. Thus, a patient who searched for a diabetes medication may start seeing advertisements for diabetes medications across their different devices and across Google.com, YouTube, YouTube TV, and non-Google websites.

146. Google, therefore, acknowledges that it uses Health Information for purposes of targeted advertising on Google Websites.

2. Google's Use of Health Information for Targeted Ads on Non-Google Websites and Apps

147. In addition to remarketing campaigns, Google enables advertisers to target ads based on user interests via "placements," "keywords," and "contextual targeting" on Non-Google Websites and Apps.

///

///

///

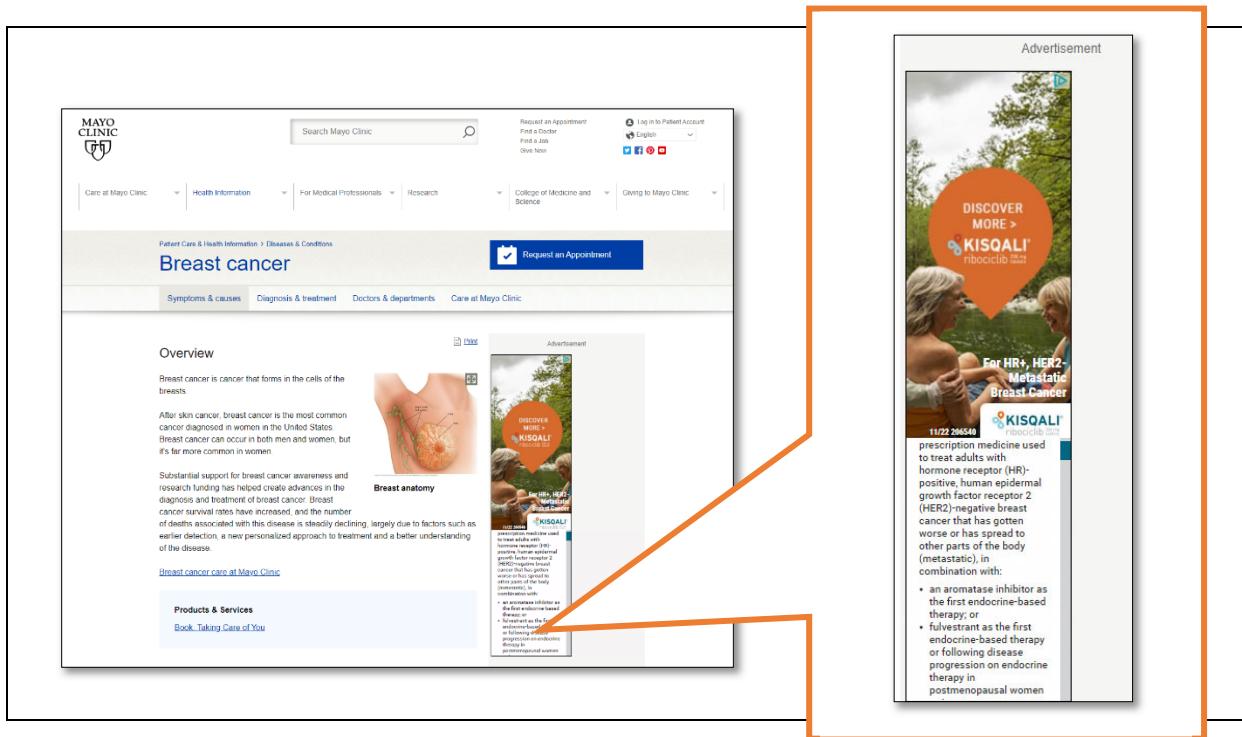
///

⁵⁰ Ex 21, *Set Up Remarketing Lists for Display Ads*, SEARCH ADS 360 HELP, at 2-3, <https://support.google.com/searchads/answer/7201620>; Ex 22, *Use Your Data Segments to Advertise on YouTube*, GOOGLE ADS HELP, at 1, <https://support.google.com/google-ads/answer/7181409>; Ex 23, *Remarketing Lists for Search Ads with Analytics*, GOOGLE ANALYTICS HELP, at 1, <https://support.google.com/analytics/answer/6212951>.

148. “Placements” help an advertiser “determine the exact URLs” where their ads appear.⁵¹ For example, an advertiser that identifies a URL where ad space is available on a property related to a Health Care Provider can choose to target ads to that specific URL.⁵²

149. In the examples below, Google served targeted “placement” ads on the Mayo Clinic web property.

150. In the first example, a pharmaceutical company has placed an ad on the Mayo Clinic “Breast Cancer” page for its “Kisqali” drug to treat “Metastatic Breast Cancer.”



///

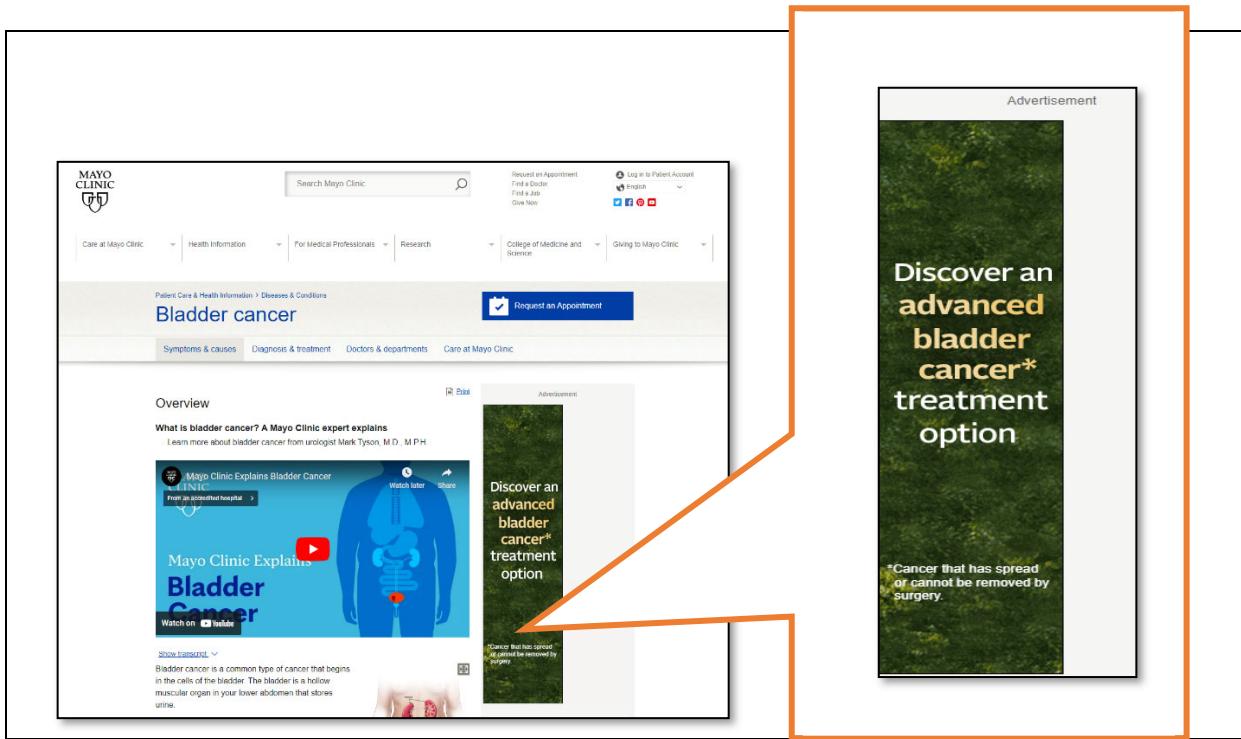
///

///

⁵¹ Ex. 24, *How Placements and Keywords Work Together*, GOOGLE ADS HELP, at 1 (archived), <http://web.archive.org/web/20230124150222/https://support.google.com/google-ads/answer/2580292>.

⁵² See generally *id.* (Ex. 24, discussing “placement”).

151. A substantially similar process appears on the “Bladder Cancer” page:



152. “Keywords” are lists of words that “determine the pages” where an advertiser’s “ad can be shown, specifically the subject or content of the page.”⁵³ “For example, if [an advertiser] wanted [its] ad to appear near content that refers to tennis, [the advertiser] could try starting with keywords related to tennis.”⁵⁴ Similar to “Placements” above, advertisers can use keywords to target users with specific health interests.

153. “Contextual Targeting” is a feature that Google provides to advertisers wherein advertisers can “match[] ads to relevant sites in [Google’s] Display [Ads] Network using your keywords or topics, among other factors.”⁵⁵ Google explains how its Contextual Targeting works:

Google’s system analyzes the content of each webpage to determine its central theme, which is then matched to [the advertiser’s] ad using [the advertiser’s]

⁵³ *Id.* (Ex. 24) at 2.

⁵⁴ *Id.* (Ex. 24).

⁵⁵ Ex. 25, *Contextual Targeting*, GOOGLE ADS HELP, at 1, <https://support.google.com/google-ads/answer/1726458>.

keywords or topic selections, [] language and location targeting, a visitor's recent browsing history, and other factors.⁵⁶

154. Thus, in each of these three scenarios, Google admits that it uses Health Information for purposes of targeted advertising on Non-Google Websites.

E. The Scope and Scale of Google's Tracking and Acquisition of Health Information

1. Google Source Code Is Present on 91 Percent of Health Care Provider Properties

155. Upon information and belief, based on investigation by counsel, an analysis of 5,297 Health Care Providers' web properties reveals that Google Source Code is present on, and thus Google is unlawfully tracking and acquiring patient Health Information from, 91 percent of the Health Care Provider web properties examined. This includes:

- a. 60 percent for Google Analytics;
- b. 59 percent for Google Ads;
- c. 50 percent for Google Display Ads;
- d. 67 percent for Google Tag Manager;
- e. 73 percent for Google APIs; and
- f. 20 percent for YouTube.

2. Google Connects Health Information Across Its Advertising Systems, Google Products and Google Properties

156. Google can amplify the Health Information that it collects in any one of its advertising systems and products by correlating and aggregating the totality of all the Health Information acquired. In this respect, Google is able to compile comprehensive and detailed Health Information profiles about individuals, and leverage these profiles in its advertising systems to make those systems more attractive to advertisers.

157. Google has integrated its advertising systems, including those described herein, to work together and share data across those systems. Thus, information Google collects through

⁵⁶ *Id.* (Ex. 25).

Google Analytics is also redirected and shared by Google across Google Ads, Google Display Ads, and YouTube, among other Google systems and products.

158. The result is an endless and pervasive process of collection and data association with individuals, including their Health Information, which enables Google to obtain unmatched insight into individuals' preferences, browsing histories, and, as relevant here, their detailed health care communications.

159. For example, and as explained further below, the Health Information that Google acquires and collects through Google Display Ads is also integrated into targeted ads served on YouTube. Google explains that it "has two properties where display ads are eligible to appear": The Google Display Network and YouTube.⁵⁷

160. In addition, Google maintains "developer" pages that explain how its different advertising systems work together and are intertwined.

161. For example, the developer pages for Google Analytics explain that Health Care Providers may link Google Analytics data to at least ten other Google advertising products through which Google collects information about consumers, which, in the case of Health Care Providers, are patients.⁵⁸ These advertising products to which Google Analytics may be linked include: Google Ads; Google AdSense; Google Ad Exchange; BigQuery; Display & Video 360; Campaign Manager 360; Search Ads 360; Postbacks; and Search Console.⁵⁹

162. For each of the products, Google provides specific instructions to developers on how to link to Google's advertising systems. For example, as set forth below, Google provides

⁵⁷ Ex. 26, *Google Display Network and YouTube on Computers, Mobile Devices, and Tablets*, GOOGLE ADS HELP, at 1, <https://support.google.com/google-ads/answer/2740623>.

⁵⁸ Ex. 2, *supra* n.8 at 7 (under the sub-heading *Designed to work together*, Google explains that advertisers should "use Analytics with other Google solutions to get a complete understanding of [their] marketing efforts and enhance performance").

⁵⁹ *Id.* (Ex. 2); *see also* Ex. 3, *supra* n.10 at 14-15, <https://marketingplatform.google.com/about/analytics-360/features/#integrations>.

specific instructions to link Google Analytics with Google Ads, Display & Video 360, and Search Ads 360.

163. Google provides the following instructions to link Google Analytics with Google Ads:



Google Ads

Google Ads is an online advertising program that helps you reach customers and grow your business. Improve your ad campaigns and analyze the entire customer journey - from ad click to conversion.

Learn more [about Google Ads](#) and how to [link your Google Analytics and Google Ads accounts](#).

[Link Google Ads](#)

164. When a developer clicks “Link Google Ads,” Google informs them that:

Configure Google Ads link group

By linking your Analytics property to your Google Ads account(s), you will enable data to flow between the products. Data exported from your Analytics property into Google Ads is subject to the Google Ads terms of service, while Google Ads data imported into Analytics is subject to the Analytics terms of service. [Learn more](#)

165. When a developer clicks “Learn more,” Google sends them to a page titled “Link/unlink Google Ads and Analytics,” where Google explains:

Link/unlink Google Ads and Analytics

Linking your Google Ads account to your Analytics property lets you see the full customer cycle, from how users interact with your marketing (e.g., seeing ad impressions, clicking ads) to how they finally complete the goals you've set for them on your site (e.g., making purchases, consuming content).

166. Google provides the following instructions to link Google Analytics with Display & Video 360:



Display & Video 360

Display & Video 360 is Google's cross-exchange real-time-bidding buying solution for large customers. The integration provides users with the ability to create remarketing audiences from within a Google Analytics 360 account and then share the audiences with a Display & Video 360 account for targeting.

Learn more about the [Display & Video 360](#) and contact your customer service rep to adjust your Display & Video 360 and Analytics account link.

167. Google provides the following instructions to link Google Analytics with Google Search Ads 360 with Google Analytics:



Search Ads 360

Search Ads 360 is a search management platform that helps agencies and marketers efficiently manage some of the largest marketing campaigns in the world across multiple engines and media channels. Integrating with your GA account allows you to see Analytics site engagement stats in Search Ads 360.

Learn more about the [Search Ads 360](#) and contact your customer service rep to adjust your Search Ads 360 and Analytics account link.

168. Further, the developer pages clearly state that the connections between Google Analytics, Google Ads, and Google Display Ads enables remarketing features:

Data Collection for Advertising Features

By enabling Advertising Features, you enable Google Analytics to collect data about your traffic in addition to data collected through a standard Google Analytics implementation. Before enabling Advertising Features, ensure that you review and adhere to the applicable policies. Data collection for remarketing also requires that data collection for advertising reporting features is enabled. [Learn more](#)

Note: By enabling the toggles below, you enable Google Analytics to automatically collect data about your traffic. If you don't want to collect data for advertising features, then you need to turn off both toggles as well as ensure that you have not manually enabled any advertising features data collection in your Google Analytics tags.

Remarketing

Enables data collection for [Display and Search Remarketing](#). This includes data from Google's signed-in users who have chosen to enable Google to associate their web and app browsing history with their Google account, and to use such information from their Google account to personalize ads. Google Analytics temporarily joins these identifiers to your Google Analytics data in order to support your audiences. When you enable this setting, you must adhere to the [Google Analytics Advertising Features Policy](#), including rules around sensitive categories and the necessary privacy disclosures to your end users about the data you collect and share with Google.

ON

///

///

///

///

///

///

///

169. The hyperlink to Display and Search Remarketing (depicted in the above screenshot) takes the developer to a page titled “About remarketing audiences in Analytics,” which explains remarketing.⁶⁰

About remarketing audiences in Analytics

Re-engage audiences that are likely to convert.

A remarketing audience is a list of cookies or mobile-advertising IDs that represents a group of users you want to re-engage because of their likelihood to [convert](#). You create remarketing audiences based on user behavior on your site or app, and then use those audiences as the basis for remarketing campaigns in your ad accounts like Google Ads and Display & Video 360.

170. This “About remarketing audiences in Analytics” page further describes how Google can use “Identifying behavior” for remarketing.⁶¹

Identifying behavior

You can use broad behavioral criteria like having simply initiated a session on your site or opened your app, or you can use more narrow criteria like interacting with specific products.

For example, you might create each of the following remarketing audiences and engage the users in them with the following kinds of ads.

Audience criteria	Ad type
Users who viewed product-detail pages, but didn't add those items to their carts	Ads for the items they didn't add to their carts
Users who added items to their carts, but didn't complete their purchases	Ads with a discount code for the items in their carts
Users who purchased items X and Y	Ads for related item Z

When a user's behavior meets the criteria you've specified, the associated cookie or Device Advertising ID is included in the audience. When any of the users with those cookies or IDs later visit sites on the Google Display Network or use Google Search, they are eligible to see one of your remarketing ads if you win the ad auction.

As you get comfortable with remarketing, you can tailor your creatives and apply [remarketing best practices](#).

⁶⁰ Ex. 27, *About Remarketing Audiences in Analytics*, GOOGLE ANALYTICS HELP, <https://support.google.com/analytics/answer/2611268>.

⁶¹ *Id.* (Ex. 27) at 1.

171. For Google Ads, Google's developer page explains that the information collected in Google Ads can be used in connection with information obtained through Google Analytics:⁶²

Google Ads remarketing tags vs. Analytics tracking code and Data Import	
<p>The Google Ads remarketing tag and the Analytics tracking code require different implementation efforts, and they each collect different data. Analytics also offers Data Import, which lets you import a wide variety of additional data beyond what you collect with the tracking code.</p> <p>In Google Ads, you build remarketing lists from the data collected by the remarketing tag. In Analytics, you build remarketing audiences from any of the data you have in Analytics. You can combine the two in a Google Ads account linked to an Analytics account.</p>	
Google Ads	Analytics
Websites: You generate an additional remarketing tag for websites, and then add the additional tag to your web pages.	Websites: You use the existing Analytics tracking code, and enable remarketing from your Analytics property settings.
Apps: You generate a remarketing ID for apps, and then add the ID to your app.	Apps: You modify the tracking code that you have included in your app.
Learn more	Learn more
You can create remarketing lists based on the following rules: Websites: <ul style="list-style-type: none">Visitors of a pageVisitors of a page who did not visit another pageVisitors of a page who also visited another pageVisitors of a page during specific datesVisitors of a page with a specific tag Apps: <ul style="list-style-type: none">All users of an appPeople who did/didn't use an app recentlyPeople using specific versions of an appPeople who took specific actions within an app	You can create remarketing audiences based on any of your Analytics data, including: <ul style="list-style-type: none">All default Analytics dataData imported from linked Google Ads accountsData imported from linked Google Marketing Platform accountsData imported via Data Import (e.g., CRM data, product meta data, custom data)
Remarketing lists are native to Google Ads.	Remarketing audiences are native to Analytics, and are shared with the linked Google Ads accounts identified in audience settings .
Google Ads tags set the advertising cookies. For example, a user without an advertising cookie comes to a site that has the Google Ads remarketing tag, the advertising cookie is set, and the user is added to the remarketing list.	Analytics tracking code tags read the advertising cookies. For example, a user without an advertising cookie comes to a site that has the Analytics remarketing-enabled tracking code, the advertising cookie is not set, and the user is not added to list.
You can use remarketing lists in Display and Search.	You can use remarketing audiences in Display and Search.

⁶² *Id.* (Ex. 27) at 3-4.

172. Google expressly acknowledges that Google Analytics can be used to facilitate remarketing on Google's search website, www.Google.com.⁶³

Remarketing Lists for Search Ads with Analytics

You can create remarketing audiences using the [Analytics tag](#), which offers sophisticated list-building capabilities. You can use these audiences with Google Ads display remarketing campaigns on the Google Display Network, or with your Google Ads search ads campaigns, to customize the campaign for people who have previously visited your site. In addition, Analytics offers detailed user analytics which can also help you decide how to create your remarketing lists.

In order to use your Analytics tag to create remarketing lists for search ads, you must [enable data collection for Remarketing features in your property settings](#). Once you have created the remarketing lists, you can associate these lists with your search ad groups.

How it works

Remarketing lists for search ads (RLSA) with Analytics works much the same way as [standard RLSA](#): you use Analytics to help define the criteria for adding customers to remarketing lists; Google associates sessions on your site (based on your Analytics criteria) with one of Google's [advertising cookies](#) on users' browsers; and when your customers later search on Google.com (from the same browser), they may see customized ads based on their previous sessions on your site.

Keep in mind:

- The maximum lifespan of a remarketing list for Google search ads is 540 days.
- A remarketing list for Google search ads must have at least 1,000 cookies before it can be used to tailor your search ads. This helps protect the privacy of those who make up your list.
- Remarketing lists that include the Google Display Network demographics dimensions Age, Gender, Interests are not eligible for RLSA.
- Remarketing lists that you create in [mobile-app views](#) are not eligible for RLSA.

Next steps

- [Enable data collection for Remarketing features in your Analytics property settings](#).
- [Create Remarketing Audiences in Analytics](#).
- [Set up remarketing lists for search ads in Google Ads](#).

173. Google provides the same "linking" functionality between its Firebase SDK and Google Ads.⁶⁴

⁶³ Ex. 23, *supra* n. 50 at 1.

⁶⁴ Ex. 28, *Link Google Ads to Firebase*, GOOGLE FIREBASE HELP, at 1-2, <https://support.google.com/firebase/answer/6383833>.

174. Google provides the following explanation for linking developer's Firebase to Google Ads:

Link Google Ads to Firebase

When you link Google Ads accounts to a Firebase project, you can

- Export Firebase events to Google Ads
- Export Firebase audiences to Google Ads

175. Once a developer links their Firebase account to Google Ads, "event data from Firebase will automatically be exported into those Google Ads accounts." Data in Google Ads can be used for each of the purposes described above.

3. Google's Tracking and Collection of Health Information Through the At-Issue Advertising Systems Are Connected Across Patient Devices

176. In addition to connecting Health Information across its advertising systems (see above), Google also connects the Health Information it obtains about patients across their different devices, browsers, and apps.

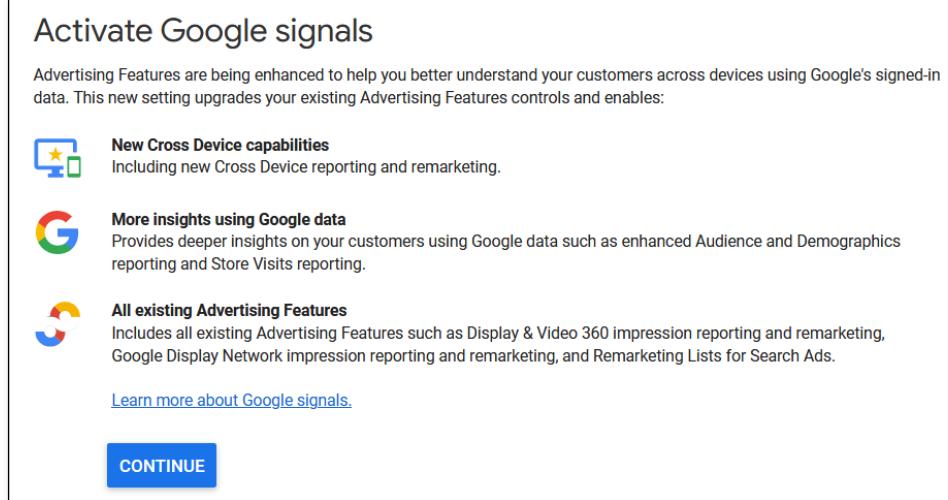
177. Specifically, if a patient owns two computing devices (e.g., a laptop and a cell phone), Google will merge, join, and co-mingle the Health Information, as well as other information it has about the patient, from one device to the other. Similarly, if a patient exchanges a communication with their Health Care Provider through a web browser and then later exchanges a communication through the Health Care Provider's app, Google can and does associate the different Health Information collected from these two different sources. Moreover, if a patient has multiple Health Care Providers from whose properties Google collects Health Information, then Google can and does collect, connect, and aggregate the Health Information concerning that patient from the patient's different Health Care Providers.

178. In each instance, Google is able to broaden its insight into the patient's Health Information and communications, more so than any single Health Care Provider.

179. Google enables cross-device connections and tracking through *at least* three different methods, which it calls “identity spaces.”⁶⁵

180. First, Google checks whether the developer has assigned its own “persistent IDs” (also called User-ID). When persistent IDs are enabled, they are intercepted alongside the data sent to Google Analytics and can be used to track the same user across multiple devices.

181. Second, Google enables cross-device connections, in part, through an advertising program called Google Signals, which is specifically intended for advertisers to “better understand [their] customers across devices using Google’s signed-in data”⁶⁶:



182. Google Signals is built into the Google Source Code and it can be easily turned on or off with a toggle.⁶⁷

///
///
///
///

⁶⁵ Ex. 29, *Reporting Identity*, GOOGLE ANALYTICS HELP, at 1, <https://support.google.com/analytics/answer/10976610>.

⁶⁶ <https://support.google.com/analytics/answer/7532985?hl=en#zippy=%2Cin-this-article>

⁶⁷ *Id.*

183. When a developer clicks “Continue,” Google sends them to a page to “Activate Google signals,” which explains:⁶⁸

Activate Google signals

Advertising Features are being enhanced to help you better understand your customers across devices using Google's signed-in data. This new setting upgrades your existing Advertising Features controls and enables:

 **New Cross Device capabilities**  **More insights using Google data**  **All existing Advertising Features**

When you choose to activate Google Signals, Google Analytics will associate the visitation information it collects from your site and/or apps with Google information from accounts of signed-in users who have consented to this association for the purpose of ads personalization. This Google information may include end user location, search history, YouTube history, and data from sites that partner with Google—and is used to provide aggregated and anonymized insights into your users' cross device behaviors. By enabling these features, you acknowledge you have the necessary privacy disclosures and rights from your end users for such association, and that such data may be accessed and/or deleted by end users via [My Activity](#). These features are also subject to the Google Analytics [Advertising Features policies](#).

Activate for **all properties** in this account.

REVIEW YOUR DATA SHARING SETTINGS

You **have not** enabled data sharing to help improve Google's products and services. The data sharing setting will also apply to authenticated visitation data collected by Google signals which is associated with Google user accounts. You acknowledge that you have the necessary rights from your end users, including disclosures in your privacy policy to share this data with Google. Enhanced Demographics and Interests Reporting is available only if you have enabled data sharing with Google. Click [here](#) to review your data sharing settings.

ACTIVATE **DECIDE LATER**

///

///

///

///

///

///

///

⁶⁸ *Id.*

184. A separate developer page provides additional details:⁶⁹

Introduction

When you activate Google signals, these existing Google Analytics features are updated to also include aggregated data from Google users who have consented to [Ads Personalization](#):

Existing Google Analytics feature	With Google signals activated
Remarketing with Google Analytics Create remarketing audiences from your Google Analytics data, and share those audiences with your linked advertising accounts.	Audiences that you create in Google Analytics and publish to Google Ads and other Google Marketing Platform advertising products can serve ads in Cross Device-eligible remarketing campaigns to Google users who have consented to Ads Personalization . Note: You need to activate Google signals in order to populate audiences that you export to YouTube. Analytics creates separate custom models for ecommerce transactions and goal completions on your site based on the cross-device conversion data from users who have signed in to their Google accounts and who have consented to Ads Personalization . Learn more about cross-device conversion exports
Advertising Reporting Features Google Analytics collects information per your measurement-code configuration, as well as Google advertising cookies that are present.	Google Analytics collects additional information about users who have consented to Ads Personalization . Learn more
Demographics and Interests reports Google Analytics collects additional information from the DoubleClick cookie (web activity) and from Device Advertising IDs	Google Analytics collects additional information about users who have consented to Ads Personalization . Learn more NOTE: If you deactivate Google signals, Analytics stops collecting this additional information. If you deactivate and then reactivate Google signals, you will have no demographic or interests information for the period during which Google signals was deactivated.
Cross Device reports (in beta) Connect data about devices and activities from different sessions so you can get an understanding of user behavior at each step of the conversion process, from initial contact to long-term retention.	Based on aggregated data from users who have consented to Ads Personalization , Google Analytics models behavior for your whole user base across device types. The data is user based rather than session based. This behavior modeling does not require User-ID views.

185. The third way Google enables cross-device connections is through “Device-ID” which is the “value from the client ID” on websites and, on apps, the “app-instance ID.”

F. Google Is Reasonably Capable of – and Does – Associate the Collected Health Information to Individual Patient Identifiers

186. Google is reasonably capable of associating, and does in fact associate, the information it acquires from Health Care Providers with specific patients and their devices.

187. The Health Information that Google unlawfully obtains is:

- a. individually identifiable health information as a matter of law under HIPAA. 45 C.F.R. § 164.514;
- b. “personal information” as a matter of law under the CCPA, Cal. Civ. Code §§ 1798.140(o), (p), (x);
- c. “Personal information” as a matter of contract under Google’s Terms of Use and Privacy Policy, which defines “personal information” as someone’s “name, email address, or billing information, or other data that can be reasonably linked to such information by Google, such as information we associated with your Google Account.”

188. Google ties the Health Information together and associates all of it together through Join IDs and identifiers that it collects across different services. These Join IDs and identifiers are tied directly to a patient’s device identifiers, geo-location, IP address, User-Agent information, and device properties that, when combined, are sufficiently unique to identify a patient, and, when they are a Google Account Holder, their specific Google Account.

189. For example, when a Google Account Holder is signed-in to their Google Account, Google acquires all of the identifiable information listed below at the same time for each service or domain listed, thereby enabling Google to link each of these identifiers with each other and also directly with: (1) the patient’s Google Account; and (2) with any other device or information that Google has already associated with that patient:

⁶⁹ *Id.*

Patient Information	Google Analytics	Google Ads	Google Display Ads
Google Account	✓	✓	✓
ga cookie / cid	✓	✓	✓
gid cookie / _gid	✓	✓	✓
Event Join IDs	✓	✓	✓
NID cookie		✓	
IDE cookie			✓
Device ID	✓	✓	✓
IP address	✓	✓	✓
User Agent	✓	✓	✓
Device Properties	✓	✓	✓
Content	✓	✓	✓

190. Google refers to an individual's Google Account ID as its "GAIA ID".

191. For signed-out Google Account Holders and Non-Google Account Holders, the only difference in the identifier collected across the different services is the name of the cookie associated with a signed-out/Non-Google Account Holders' device.

192. For Google Ads, the signed-out browser identifier is the NID cookie, which Google internally refers to as a "Zwieback ID" and is:

- used to show Google ads in Google services for signed-out users;
- used to acquire information about patient activity on Health Care Provider and covered entity digital properties;
- used to uniquely identify a patient's device and browser;
- acquired by Google when a user is signed-in to a Google Account and when they are not signed-in to a Google Account; and
- a value for which Google is reasonably capable of associating with a patient's Google Account and their Health Information.

193. For Google Display Ads, the signed-out browser identifier is the IDE cookie, which is internally referred to as a "Biscotti ID" and is:

- used to show Google ads on non-Google sites;
- used to acquire information about patient activity on Health Care Provider and covered entity digital properties;
- used to uniquely identify a patient's device and browser;

- d. acquired by Google when a user is signed-in to a Google Account and when they are not signed-in to a Google Account; and
- e. a value for which Google is reasonably capable of associating with a patient's Google Account and their Health Information.

194. As a result of Google acquiring the Google Account cookies and the signed-out browser identifier cookies at the same time, Google correlates the signed-out browser identifying cookies for Google Analytics, Google Ads, and Google Display Ads (among other products) with specific Google Account Holders any time that Google collects the signed-out browser identifying cookie – and then also with any other information that Google has collected about the Account holder through any other Google consumer or business service.

195. As a result of acquiring Google Account identifiers alongside each of these other identifiers or identifying properties, Google is reasonably capable of associating and does in fact associate each of the other identifiers or identifying properties with specific patients via their Google Accounts.

196. For example, if on Monday, Google acquires Patient Jane Doe's Google Account ID alongside all of the other identifiers in the chart above, Google is reasonably capable of linking and links all of the other identifiers in the chart to Jane Doe's Google Account ID. Then, if Jane Doe exchanges communications with her Health Care Provider using the same device on Tuesday, Google will be reasonably capable of associating Jane Doe's activity on Tuesday with her activity on Monday, regardless of whether Google acquires Jane Doe's Google Account ID directly with the activity she conducted on Tuesday.

197. Google's association of the information it collects from non-Google web-properties (such as the Health Care Properties here) is actual and widespread, not theoretical.

198. Google maintains a data system with "proto files" that "shows that Google commingles signed-in and signed-out information" together in various columns. One such column involves co-mingling data in the categories that include but are not limited to GAIA ID, Biscotti ID, Zwieback ID, PPID, Device ID, First Party User IDs, Buyside Publisher ID, Publisher User

IDs, DUIS, YouTube Visitor ID, precise geo-coordinates, areas-of-interest, shipping address, credit card information, household income, age, gender, race, ethnicity, children, and education.

199. Google also maintains numerous files that contain GAIA, Biscotti, and/or Zwieback alongside each other or with an “identifier that can be used to bridge Gaia, Biscotti, and Zwieback ID spaces,” such as device IDs like an Android ID or iOS IDFA; or contain “high entropy fields, which when combined together could be sufficient to uniquely identify users alongside GAIA, Biscotti, or Zwieback,” including “fields [i.e. information categories] representing various types of fingerprints to uniquely identify users” such as browser-fingerprinting, Picasso fingerprinting, and font fingerprinting.

200. The document filed in this action at Dkt. 61-8 also indicates that Google stores additional information alongside the GAIA, Biscotti, or Zwieback identifiers.

201. A Google employee has publicly stated that Google maintains tables that “contain mappings between Google Analytics User ID (UID) or client ID (CID) and Biscotti” as well as “mappings between UID or CID and device ID received from App events.” This document was filed in this action at Dkt. 61-4.

202. As a result of these and other potential mappings, the Google Analytics identifiers are not actually “pseudonymous” in any way because they are linked to unique, persistent identifiers that directly identify specific devices and households and are also linked to a patient’s Google Account, precise geo-location, and as yet unknown identifying information that potentially includes a user’s phone number (see Dkt. 61 ¶ 30c.).

203. Google measures ad conversions “through mapping a GAIA ID to a Biscotti ID.” Dkt. 61 ¶ 30b.

G. Google Can Identify the Health Care Providers From Which It Unlawfully Acquired Health Information

204. Google is able to identify the Health Care Providers from which it unlawfully acquired Health Information.

205. Google can readily identify the web properties which use the Google Source Code.

206. In addition, for those web properties that use the Google Source Code, Google has tools that it uses in the ordinary course of its business that it can easily use to identify the web properties that are Health Care Providers (as defined herein). This includes using (1) its search index spider to identify health care properties with key terms required by law and (2) content categorizations that Google has publicly stated it has applied to web properties. Plaintiffs address each in turn.

207. Federal law requires every health care provider or covered entity under HIPAA to “prominently post its [HIPAA] notice on the website and make the notice electronically available through the website.” 45 C.F.R. § 164.520(c)(3).

208. Federal law further specifies that each HIPAA notice is required to include the phrase:

“THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THAT INFORMATION.”

45 C.F.R. § 164.520(b)(1)(i).

209. Google publicly explains that “most of [its] Search index is built through the work of software known as crawlers [that] automatically visit publicly accessible webpages and follow links on those pages.⁷⁰ Google further explains that when its crawlers review a webpage Google’s “systems render the content of the page, just as a browser does” and Google then “take[s] note of key signals,” including “keywords” about the page.⁷¹ “The Google Search index contains hundreds of billions of webpages and is well over 100,000,000 gigabytes in size. It’s like the index in the back of a book – with an entry for every word seen on every webpage we index.”⁷²

210. Google describes the crawling process and what happens next in further detail:⁷³

⁷⁰ Ex. 30, *Organizing Information - How Google Search Works*, GOOGLE SEARCH, at 2, <https://www.google.com/search/howsearchworks/how-search-works/organizing-information>.

⁷¹ *Id.* (Ex. 30).

⁷² *Id.* (Ex. 30).

⁷³ Ex. 31, *In-depth Guide to How Google Search Works*, GOOGLE SEARCH CENTRAL, at 2, <https://developers.google.com/search/docs/fundamentals/how-search-works>.

After a page is crawled, Google tries to understand what the page is about. This stage is called indexing and it includes processing and analyzing the textual content and key content tags and attributes, such as <title> elements and alt attributes, images, videos, and more.

211. Therefore, Google can readily identify all or substantially all Health Care Providers from which it is acquiring Health Information by using the Google crawlers to identify and index all properties that include a HIPAA notice.

212. Similarly, to identify pharmaceutical companies subject to medical privacy laws, Google can use its crawlers to identify properties that have pharmaceutical warnings required by the FDA to market prescription drugs.

213. The regulation on Medication Guides for Prescription Drug Products “sets forth [the] requirements for patient labeling for human prescription drug products ... that the [FDA] determines pose a serious and significant public health concern requiring distribution of FDA-approved patient information.” 21 C.F.R. § 208.1(a). “The purpose of patient labeling for human prescription drug products ... is to provide information when the FDA determines in writing that it is necessary to patients’ safety and effective use of drug products.” *Id.*

214. Under 21 C.F.R. § 208.20, a “Medication Guide” “shall contain” a series of “headings relevant to the drug product” which “shall contain the specific information as follows: ... (1) [t]he brand name; (2) the heading, ‘What is the most important information I should know about (name of drug)?’ followed by a statement describing the particular serious and significant public health concern that created the need for the Medication Guide ...”; and (3) “the heading ‘What is (name of drug)?’ followed by a section that identifies a drug product’s indications for use” and other phrases.

215. Prescription drug web properties typically include Medication Guide information.

216. Therefore, Google can readily identify all or substantially all pharmaceutical companies from which it is acquiring Health Information by using the Google crawlers to identify and index all properties that include the Medication Guide information.

217. In addition to “indexing” the legally required language on web properties, Google and other data industry companies categorize webpage and/or web property “content” into

classifications or taxonomies (sometimes referred to as “verticals”) that are typically used for ad targeting.

218. Industry “Content Taxonomy” standards are published by the Interactive Advertising Bureau (IAB), a trade group consisting of more than 700 companies that develops technical standards and solutions for the ad tech industry.⁷⁴ The IAB “Content Taxonomy” standards include, but are not limited to, the following categories: medical health, blood disorders, bone and joint conditions, brain and nervous system disorders, cancer, dental health, diabetes, digestive disorders, ENT conditions, endocrine and metabolic diseases, hormonal disorders, menopause, thyroid disorders, eye and vision conditions, foot health, heart and cardiovascular diseases, infectious diseases, lung and respiratory health, mental health, reproductive health, birth control, infertility, pregnancy, sexual health, skin and dermatology, sleep disorders, substance abuse, medical tests, pharmaceutical drugs, surgery, and vaccines.

219. Google has publicly listed verticals that it employs or has employed internally to categorize the content of particular communications and/or web properties. This is available at <https://developers.google.com/adwords/api/docs/appendix/verticals> and includes the following health categories:

Criterion ID	Parent ID	Category
249	38	/Finance/Insurance/Health Insurance
45	0	/Health
623	45	/Health/Aging & Geriatrics
624	623	/Health/Aging & Geriatrics/Alzheimer's Disease
499	45	/Health/Alternative & Natural Medicine
1239	499	/Health/Alternative & Natural Medicine/Acupuncture & Chinese Medicine
1238	499	/Health/Alternative & Natural Medicine/Cleansing & Detoxification
419	45	/Health/Health Conditions
625	419	/Health/Health Conditions/AIDS & HIV
626	419	/Health/Health Conditions/Allergies
628	419	/Health/Health Conditions/Arthritis
630	419	/Health/Health Conditions/Blood Sugar & Diabetes
429	419	/Health/Health Conditions/Cancer
629	419	/Health/Health Conditions/Cold & Flu

⁷⁴ The full standards are available at: <https://iabtechlab.com/standards/content-taxonomy> (last visited Nov. 13, 2023).

Criterion ID	Parent ID	Category
1211	419	/Health/Health Conditions/Ear Nose & Throat
571	419	/Health/Health Conditions/Eating Disorders
1328	419	/Health/Health Conditions/Endocrine Conditions
1329	1328	/Health/Health Conditions/Endocrine Conditions/Thyroid Conditions
638	419	/Health/Health Conditions/GERD & Digestive Disorders
941	419	/Health/Health Conditions/Genetic Disorders
559	419	/Health/Health Conditions/Heart & Hypertension
643	559	/Health/Health Conditions/Heart & Hypertension/Cholesterol Issues
632	419	/Health/Health Conditions/Infectious Diseases
1262	632	/Health/Health Conditions/Infectious Diseases/Parasites & Parasitic Diseases
1263	632	/Health/Health Conditions/Infectious Diseases/Vaccines & Immunizations
817	419	/Health/Health Conditions/Injury
942	419	/Health/Health Conditions/Neurological Conditions
641	942	/Health/Health Conditions/Neurological Conditions/Learning & Developmental Disabilities
642	641	/Health/Health Conditions/Neurological Conditions/Learning & Developmental Disabilities/ADD & ADHD
1856	641	/Health/Health Conditions/Neurological Conditions/Learning & Developmental Disabilities/Autism Spectrum Disorders
818	419	/Health/Health Conditions/Obesity
819	419	/Health/Health Conditions/Pain Management
631	819	/Health/Health Conditions/Pain Management/Headaches & Migraines
824	419	/Health/Health Conditions/Respiratory Conditions
627	824	/Health/Health Conditions/Respiratory Conditions/Asthma
420	419	/Health/Health Conditions/Skin Conditions
633	419	/Health/Health Conditions/Sleep Disorders
254	45	/Health/Health Education & Medical Training
252	45	/Health/Health Foundations & Medical Research
251	45	/Health/Medical Devices & Equipment
1352	251	/Health/Medical Devices & Equipment/Assistive Technology
1353	1352	/Health/Medical Devices & Equipment/Assistive Technology/Mobility Equipment & Accessories
256	45	/Health/Medical Facilities & Services
634	256	/Health/Medical Facilities & Services/Doctors' Offices
250	256	/Health/Medical Facilities & Services/Hospitals & Treatment Centers
635	256	/Health/Medical Facilities & Services/Medical Procedures
943	635	/Health/Medical Facilities & Services/Medical Procedures/Medical Tests & Exams
944	635	/Health/Medical Facilities & Services/Medical Procedures/Surgery
238	944	/Health/Medical Facilities & Services/Medical Procedures/Surgery/Cosmetic Surgery
500	256	/Health/Medical Facilities & Services/Physical Therapy
253	45	/Health/Medical Literature & Resources
945	253	/Health/Medical Literature & Resources/Medical Photos & Illustration
636	45	/Health/Men's Health
437	45	/Health/Mental Health
639	437	/Health/Mental Health/Anxiety & Stress
511	437	/Health/Mental Health/Counseling Services

Criterion ID	Parent ID	Category
640	437	/Health/Mental Health/Depression
418	45	/Health/Nursing
649	418	/Health/Nursing/Assisted Living & Long Term Care
456	45	/Health/Nutrition
457	456	/Health/Nutrition/Special & Restricted Diets
1572	457	/Health/Nutrition/Special & Restricted Diets/Kosher Foods
1570	457	/Health/Nutrition/Special & Restricted Diets/Low Carbohydrate Diets
1571	457	/Health/Nutrition/Special & Restricted Diets/Low Fat & Low Cholesterol Diets
237	456	/Health/Nutrition/Vitamins & Supplements
245	45	/Health/Oral & Dental Care
645	45	/Health/Pediatrics
248	45	/Health/Pharmacy
646	248	/Health/Pharmacy/Drugs & Medications
947	45	/Health/Public Health
1256	947	/Health/Public Health/Health Policy
644	947	/Health/Public Health/Occupational Health & Safety
946	947	/Health/Public Health/Toxic Substances & Poisoning
195	45	/Health/Reproductive Health
198	195	/Health/Reproductive Health/Birth Control
647	195	/Health/Reproductive Health/Infertility
202	195	/Health/Reproductive Health/Male Impotence
558	195	/Health/Reproductive Health/OBGYN
536	195	/Health/Reproductive Health/Sex Education & Counseling
1236	195	/Health/Reproductive Health/Sexual Enhancement
421	195	/Health/Reproductive Health/Sexually Transmitted Diseases
257	45	/Health/Substance Abuse
1351	257	/Health/Substance Abuse/Drug & Alcohol Testing
1350	257	/Health/Substance Abuse/Drug & Alcohol Treatment
1237	257	/Health/Substance Abuse/Smoking & Smoking Cessation
1235	257	/Health/Substance Abuse/Steroids & Performance-Enhancing Drugs
246	45	/Health/Vision Care
1502	246	/Health/Vision Care/Eye Exams & Optometry
1224	246	/Health/Vision Care/Eyeglasses & Contacts
1503	246	/Health/Vision Care/Laser Vision Correction
648	45	/Health/Women's Health

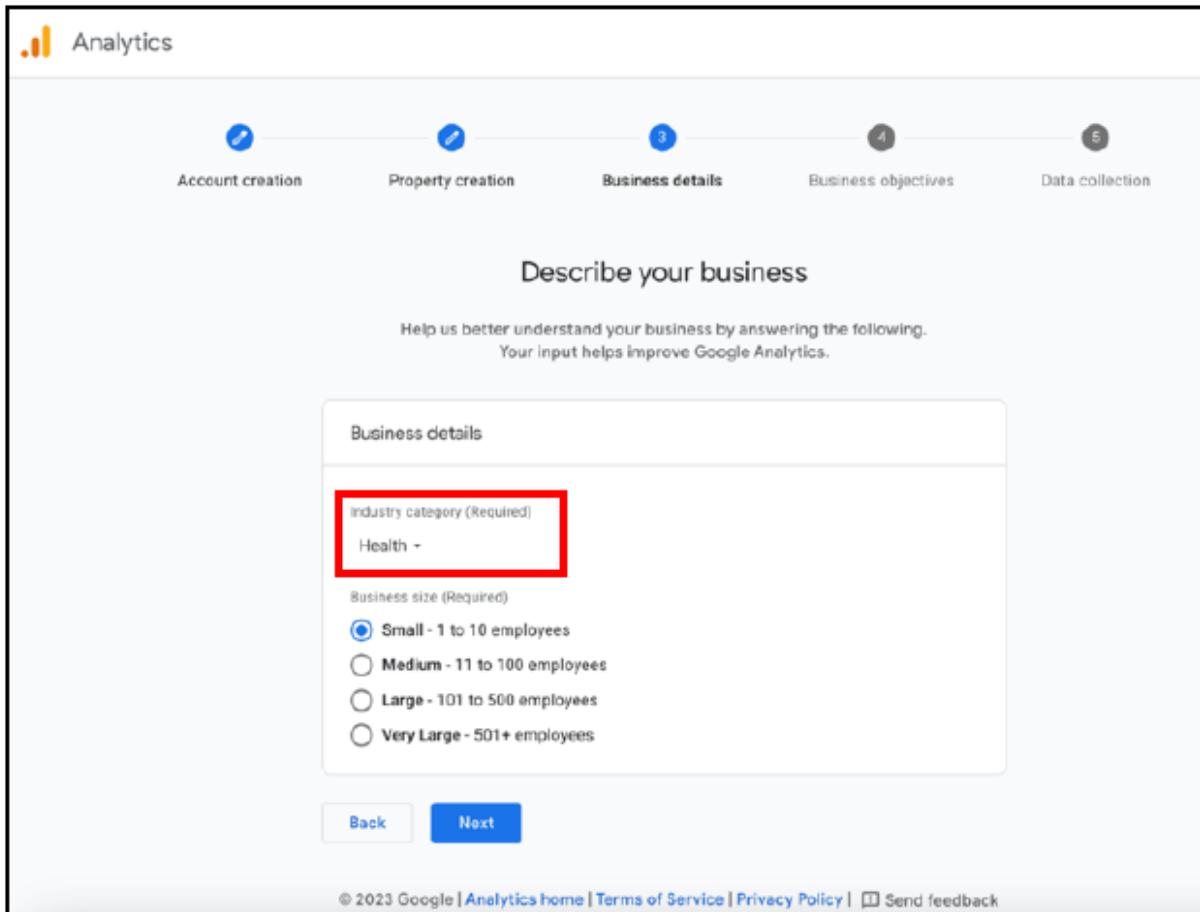
220. Therefore, Google can readily identify all or substantially all Health Care Providers from which it is acquiring Health Information by using its existing content taxonomy to filter for health-related information.

///

///

///

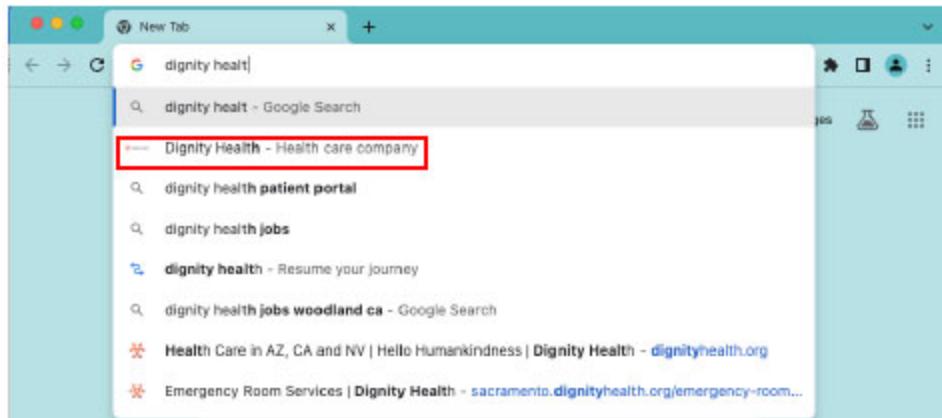
221. Google also collects information about the nature of business or entities using the Analytics. In the sign-up process, Google Analytics requires users to fill in a field named “industry category” where one of the choices is “Health”:



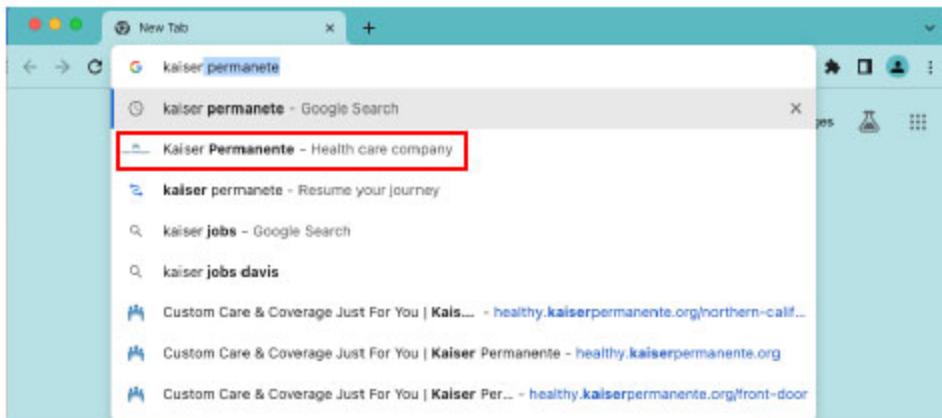
The screenshot shows the 'Business details' step of the Google Analytics sign-up process. The step is numbered 3. The 'Industry category' field is highlighted with a red box and contains the value 'Health'. Below the field, there are four radio button options for 'Business size': 'Small - 1 to 10 employees' (selected), 'Medium - 11 to 100 employees', 'Large - 101 to 500 employees', and 'Very Large - 501+ employees'. At the bottom of the step, there are 'Back' and 'Next' buttons, and a copyright notice: '© 2023 Google | [Analytics home](#) | [Terms of Service](#) | [Privacy Policy](#) | [Send feedback](#)'.

///
///
///
///
///
///
///
///
///

222. The Google Chrome browser also has tools that categorize web-properties as being health care companies. For example, the autocomplete feature in Chrome is able to identify a health care provider before a user types in the full website address:



Dignity Health – “Health care company”



Kaiser Permanente – “Health care company”

223. Accordingly, Google is readily capable of identifying the Health Care Providers from whom it has unlawfully acquired Health Information because: (1) Google knows which web properties are using the Google Source Code; and (2) Google can cross-reference that list for Health Care Providers because it has existing systems of indexing and content categorization.

224. This knowledge that it is collecting Health Information also demonstrates that Google's conduct is knowing and intentional. If Google wished to do so, it could stop collecting the illicit Health Information. However, it does not do so because its collection permits Google to

obtain significant profits from the Health Information collected about patients without their knowledge or authorization.

H. Google's Acquisition and Its Own Use of Health Information Is Unlawful and Violates Reasonable Expectations of Privacy

225. As set forth below, Google's acquisition of Health Information is unlawful because Google's possession of this information, and thus by extension its internal use, violates federal, state and common law, which protects the disclosure of Health Information and which requires valid patient consent – something Google does not have.

226. In addition, Google's acquisition and internal use of Health Information constitutes an invasion of privacy as individuals have a reasonable expectation of privacy over their Health Information. This includes reasonable expectations of privacy that:

- a. Their Health Information will not be tracked by Google without their express knowledge and authorization;
- b. Their Health Information will not be collected by Google without their express knowledge and authorization;
- c. Their Health Information will not be monetized by Google without their express knowledge and authorization;
- d. Their Health Information will not be used for any marketing purpose by Google without their express knowledge and authorization;
- e. Google will not permit or enable Health Care Providers to use Google tools in a way through which Google can track, collect, and monetize their Health Information; and
- f. Google will not knowingly participate in or enable unlawful activity that negatively impacts their rights, either on its own or in coordination with their Health Care Providers.

227. These expectations of privacy are well-grounded, as the confidentiality, sensitivity and inherent privacy of Health Information have been recognized and held firm throughout history

and within current legal frameworks. Indeed, the confidentiality of Health Information finds its origins as far back as 400 B.C., in the original Hippocratic Oath:

Whatever I see or hear in the lives of my patients, whether in connection with my professional practice or not, which ought not to be spoken of outside, I will keep secret, as considering all such things to be private.⁷⁵

228. That Oath is embodied today in the legal concept of a medical provider's duty of confidentiality. *See, e.g.*, American Medical Association's ("AMA") Code of Medical Ethics Opinion 3.1.1. (affirming that "protecting information gathered in association with the care of the patient is a core value in health care" and "[p]atient privacy encompasses a number of aspects including...personal data (informational privacy . . .)" . . ."Physicians must seek to protect patient privacy in all settings to the greatest extent possible...");⁷⁶ AMA Code of Medical Ethics Opinion 3.2.4 (confirming expectation of privacy over health-related information and stating that third-party access for commercial purposes can only occur if information has been de-identified and with full disclosure to patients);⁷⁷ AMA Code of Medical Ethics Opinion 3.3.2 (same)⁷⁸.

229. The protections afforded Health Information are also well-recognized in federal, state and common law. Each is addressed in turn below.

1. Google's Conduct Is Unlawful and Individuals Have a Reasonable Expectation of Privacy Under Federal Law

230. Google's unlawful acquisition and use of Health Information for which an individual has a reasonable expectation of privacy is well supported by federal law.

231. Health Information Portability and Accountability Act (HIPAA): HIPAA provides federal protections for "protected health information," which includes the Health Information at issue in this case.

⁷⁵ Michael North, *Translation of Original Hippocratic Oath*, NAT'L LIBR. OF MED., at 2, https://www.nlm.nih.gov/hmd/greek/greek_oath.html (last visited Nov. 13, 2023).

⁷⁶ Ex. 32, *Privacy in Health Care: Code of Medical Ethics Opinion 3.1.1*, AM. MED. ASS'N, <https://code-medical-ethics.ama-assn.org/sites/default/files/2022-08/3.1.1.pdf>.

⁷⁷ Ex. 33, *Access to Medical Records by Data Collection Companies: Opinion 3.2.4*, AM. MED. ASS'N, <https://code-medical-ethics.ama-assn.org/sites/default/files/2022-08/3.2.4.pdf>.

⁷⁸ Ex. 34, *Confidentiality & Electronic Medical Records: Code of Medical Ethics Opinion 3.3.2*, AM. MED. ASS'N, <https://code-medical-ethics.ama-assn.org/sites/default/files/2022-08/3.3.2.pdf>

232. Specifically, “protected health information” is defined to include “individually identifiable health information” that is transmitted or maintained by electronic media or in any other form or medium. 45 C.F.R. § 160.103. Any person (e.g. Google) who knowingly and in violation of HIPAA: “(1) uses or causes to be used a unique health identifier; (2) obtains individually identifiable health information relating to an individual; or (3) discloses individually identifiable health information to another person” may be subject to fines and imprisonment. 42 U.S.C. § 1320d-6.⁷⁹

233. “Individually identifiable health information” is, in turn, broadly defined to include electronic information and to mean:

any information, including demographic information, collected from an individual that is:

- (A) created or received by a [Health Care Provider]; and
- (B) relates to the past, present or future physical or mental health condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and
 - (i) identifies the individual; or
 - (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

See 42 U.S.C. § 1320(6); see also 45 C.F.R. 160.103.

234. This definition squarely encompasses the Health Information at issue, which includes the specific actions taken by patients on their Health Care Provider web properties, the specific time and frequency of each patient interaction (e.g., specific information about when a patient logs-in and logs-out of an online patient portal, requests an appointment, or seeks information about a specific doctor, condition, treatment, or prescription drug) and the content of

⁷⁹ While there is no private right of action under HIPAA, it nonetheless provides support for the conclusion that Google’s conduct is unlawful and an invasion of privacy. Indeed, as discussed further below, HIPAA and its corresponding regulations provide on-point guidance as to the illegality of the conduct alleged herein.

communications that patients exchange with their Health Care Providers, including communications related to specific medical conditions.⁸⁰

235. Likewise, with respect to what “identifies the individual,” HIPAA’s corresponding federal regulations clarify that “identifiers” are broadly interpreted to include “any [] unique identifying number, characteristic or code...” (42 CFR 164.514(b)(2)(i)(R)), e.g., the identifiers that are at issue in this case.

236. The above scope and framework of HIPAA clearly reflects the public policy to protect, and indeed the public expectation of privacy over, the Health Information at issue in this case.

237. And lest there be any dispute, HHS issued a bulletin in December 2022 confirming that use of tracking technologies, such as the Google Source Code, which “collect and analyze information about how internet users are interacting with a regulated entity’s website or mobile application[,]” are improper for Health Care Provider web properties.⁸¹ Critically, this bulletin did

⁸⁰ In fact, guidance from the U.S. Department of Health and Human Services (“HHS”) (charged with enforcing and rulemaking under HIPAA), confirms that patient status, *alone*, is protected health information. Ex. 35, *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the HIPAA Privacy Rule*, U.S. DEP’T OF HEALTH AND HUM. SERV., at 5 (Nov. 26, 2012), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf (confirming that “[i]f such information was listed with health condition, health care provision or payment data, such as *an indication that the individual was treated at a certain clinic*, then this information would be [protected health information]”) (emphasis added); *see also* Ex. 36, *Marketing*, U.S. DEP’T OF HEALTH AND HUM. SERV., at 2 (Rev. Apr. 3, 2003), <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf> (“covered entities may not sell lists of patients . . . to third parties without obtaining authorization from each person on the list”); 65 Fed. Reg. 82717 (Dec. 28, 2000) (stating the “sale of a patient list to a marketing firm” is not permitted under HIPAA); 67 Fed. Reg. 53186 (Aug. 14, 2002) (requiring that “[a] covered entity must have the individual’s prior written authorization to use or disclose protected health information for marketing communications,” which includes disclosure of patient status through a patient list); 78 Fed. Reg. 5642 (Jan. 25, 2013) (finding that it would be a HIPAA violation “if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers”).

⁸¹ Ex. 37, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. DEP’T OF HEALTH AND HUM. SERV., at 1 (Dec. 1, 2022), <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>.

not create new obligations but rather “highlight[ed]” existing obligations under HIPAA, providing and relying on previous guidance and rules that have been in place for decades.

238. As relevant here, the bulletin highlighted the following:

a. The bulletin confirmed that use of tracking technologies on a Health Care Provider’s website or app results in the disclosure of individually identifiable health information and thus falls within the protections of HIPAA. The bulletin explains:

Regulated entities disclose a variety of information to tracking technology vendors through tracking technologies placed on a regulated entity’s website or mobile app, including individually identifiable health information (IIHI) that the individual provides when they use regulated entities’ websites or mobile apps. This information might include an individual’s medical record number, home or email address, or dates of appointments, as well as an individual’s IP address or geographic location, medical device IDs, or any unique identifying code. All such IIHI collected on a regulated entity’s website or mobile app generally is [protected health information (PHI)], even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services. This is because, when a regulated entity collects the individual’s IIHI through its website or mobile app, the information connects the individual to the regulated entity (i.e. it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual’s past, present, or future health or health care or payment for care.⁸²

b. The bulletin confirmed tracking technology vendors, e.g. Google, must also be subject to HIPAA when protected health information is at issue. In such cases, Health Care Providers are required to enter into a business associate agreement (BAA) with the vendor to ensure that protected health information is protected in accordance with HIPAA. The bulletin explains:

[] [T]racking technology vendors are business associates if they create, receive, maintain, or transmit PHI on behalf of a regulated entity for a covered function (e.g. health care operations) or provide certain services to or for a covered entity (or another business associate) that involve the disclosure of PHI. In these circumstances,

⁸² *Id.* (Ex. 37) at 4 (explanation provided under sub-heading “How do the HIPAA Rules apply to regulated entities’ use of tracking technologies?”) (internal citations omitted).

regulated entities must ensure that the disclosures made to such vendors are permitted by the Privacy Rule and enter into a business associate agreement (BAA) with these tracking technology vendors to ensure that PHI is protected in accordance with the HIPAA Rules. For example, if an individual makes an appointment through the website of a covered health clinic for health services and that website uses third party tracking technologies, then the website might automatically transmit information regarding the appointment and the individual's IP address to a tracking technology vendor. In this case, the tracking technology vendor is a business associate and a BAA is required.⁸³

- c. The bulletin confirmed that use of tracking technologies on "authenticated" webpages, i.e., pages which require log-on (like a patient portal), implicates HIPAA protections. The bulletin explains:

Regulated entities may have user-authenticated webpages, which require a user to log in before they are able to access the webpage, such as a patient or health plan beneficiary portal or a telehealth platform. Tracking technologies on a regulated entity's user-authenticated webpages generally have access to PHI. Such PHI may include, for example, an individual's IP address, medical record number, home or email addresses, dates of appointments, or other identifying information that the individual may provide when interacting with the webpage. Tracking technologies within user-authenticated webpages may even have access to an individual's diagnosis and treatment information, prescription information, billing information, or other information within the portal. Therefore, a regulated entity must configure any user-authenticated webpages that include tracking technologies to allow such technologies to **only** use and disclose PHI in compliance with the HIPAA Privacy Rule and must ensure that the electronic protected health information (ePHI) collected through its website is protected and secured in accordance with the HIPAA Security Rule.⁸⁴

- d. The bulletin confirmed that use of tracking technologies on "unauthenticated" webpages likely implicates HIPAA protections. The bulletin explains that while tracking on unauthenticated webpages may not have access to individuals' PHI, this is not always the case:

[[T]racking technologies on unauthenticated webpages may have access to PHI, in which case the HIPAA Rules apply to the regulated

⁸³ *Id.* (Ex. 37) at 5 (explanation provided under sub-heading "Tracking on user-authenticated webpages") (internal citations omitted).

⁸⁴ *Id.* (Ex. 37) at 4-5 (explanation provided under sub-heading "Tracking on user-authenticated webpages") (bold emphasis in original) (internal citations omitted).

entities' use of tracking technologies and disclosures to tracking technology vendors. Examples of unauthenticated webpages where the HIPAA Rules apply include:

- The login page of a regulated entity's patient portal (which may be the website's homepage or a separate, dedicated login page), or a user registration webpage where an individual creates a login for the patient portal, generally are unauthenticated because the individual did not provide credentials to be able to navigate to those webpages. However, if the individual enters credential information on that login webpage or enters registration information (e.g., name, email address) on that registration page, such information is PHI. [Footnote.] Therefore, if tracking technologies on a regulated entity's patient portal login page or registration page collect an individual's login information or registration information, that information is PHI and is protected by the HIPAA Rules.
- Tracking technologies on a regulated entity's unauthenticated webpage that addresses specific symptoms or health conditions, such as pregnancy or miscarriage, or that permits individuals to search for doctors or schedule appointments without entering credentials may have access to PHI in certain circumstances. For example, tracking technologies could collect an individual's email address and/or IP address when the individual visits a regulated entity's webpage to search for available appointments with a health care provider. In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.⁸⁵

e. The bulletin confirms that Health Care Providers must ensure that proper notice and consent are acquired for the disclosure of protected health information.

The bulletin explains:

...

- Regulated entities may identify the use of tracking technologies in their website or mobile app's privacy policy, notice, or terms and conditions of use. However, the Privacy Rule does **not** permit disclosures of PHI to a tracking technology vendor [e.g. Google] based solely on a regulated entity informing individuals in its privacy policy, notice, or terms and conditions of use that it plans to make such disclosures. Regulated entities must ensure that all tracking technology vendors have signed a BAA and that there is an applicable permission prior to a disclosure of PHI.
- If there is not an applicable Privacy Rule permission or if the vendor is not a business associate of the regulated entity, then the individual's HIPAA-compliant authorizations are required

⁸⁵ *Id.* (Ex. 37) at 5-6 (explanation provided under sub-heading "Tracking on unauthenticated webpages") (internal citations omitted).

before the PHI is disclosed to the vendor. Website banners that ask users to accept or reject a website's use of tracking technologies, such as cookies, do **not** constitute a valid HIPAA authorization.

- Further, it is insufficient for a tracking technology vendor to agree to remove PHI from the information it receives or de-identify the PHI before the vendor saves the information. Any disclosure of PHI to the vendor without individuals' authorizations requires the vendor to have a signed BAA in place **and** requires that there is an applicable Privacy Rule permission for disclosure.⁸⁶

239. Given the above framework, it is clear that HIPAA protections encompass the conduct and Health Information at issue here. Google's acquisition and use of patients' Health Information is unlawful and individuals have an objectively reasonable expectation of privacy over this information.

240. The FTC Act: As pertains to this case, the Federal Trade Commission has stated that under federal consumer protection law "health information" is "anything that conveys information – or enables an inference – about a consumer's "health" and provides an example that location-data alone (such as "repeated trips to a cancer treatment facility") "may convey highly sensitive information about consumer's health."⁸⁷

241. The FTC has joined with HHS in warning that sharing HIPAA-covered information or FTC Act "health information" with Google is an unfair business practice. In the words of Samuel Levine, Director of the FTC's Bureau of Consumer Protection, "[w]hen consumers visit a hospital's website or seek telehealth services, they should not have to worry that their most private

⁸⁶ *Id.* (Ex. 37) at 7-8 (explanation provided under sub-heading, "HIPAA compliance obligations for regulated entities when using tracking technologies") (bold emphasis in original) (internal citations omitted).

⁸⁷ Ex. 38, Elisa Jillson, *Protecting the Privacy of Health Information: A Baker's Dozen Takeaways from FTC Cases*, FED. TRADE COMM'N BUSINESS BLOG, at 1 (July 25, 2023), <https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases>, July 25, 2023.

and sensitive health information may be disclosed to advertisers and other unnamed, hidden third parties.”⁸⁸

242. In July 2023, the FTC and HHS sent a “joint letter to approximately 130 hospital systems and telehealth providers to alert them about the risks and concerns about the use of technologies, such as … Google Analytics, that can track a user’s online activities. These tracking technologies gather identifiable information about users, usually without their knowledge and in ways that are hard for users to avoid, as users interact with a website or mobile app.”⁸⁹

243. The FTC and HHS Joint Letter sought to “draw … attention to serious privacy and security risks related to the use of online tracking technologies” present on Healthcare Provider websites and apps that “impermissibly disclos[e] consumers’ sensitive health information to third parties,” including Google. The FTC pointed out that companies have obligations to protect “health information” even if they “are not covered by HIPAA.”⁹⁰

244. The Electronic Communications Privacy Act (“ECPA”): While not specific to Health Information, the ECPA provides guiding standards for the protection of electronic communications, which are at issue in this action. Under the ECPA, Google cannot intercept, acquire and/or use the “content” of an electronic communication, i.e. the substance, purport, or meaning of an electronic communication, without the lawful consent of a party to a communication. See 18 U.S.C. § 2511(1), (2)(d).⁹¹

⁸⁸ Ex. 39, *FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies*, FED. TRADE COMM’N, at 1 (July 20, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking>.

⁸⁹ *Id.* (Ex. 39) at 2.

⁹⁰ Ex. 40, *HHS and FTC Joint Letter to Third Party Trackers*, FED. TRADE COMM’N, at 1-2 (July 20, 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf.

⁹¹ Google did not obtain lawful consent from Plaintiffs and Class Members. Further, insofar as Google contends that consent was obtained from the Health Care Provider, such consent is invalid for the purposes of the ECPA because it was acquired “for the purpose of committing [] criminal or tortious act[s] in violation of the Constitution or laws of the United States or of any State” (18 U.S.C. § 1251(2)(d)), including but not limited to violation of the laws set forth herein.

245. The Health Information at issue in this action pertains to the substance, purport or meaning of patients' electronic health communications because it includes, but is not limited to, interception and acquisition by Google of the specific actions taken by patients on their Health Care Provider web properties, the specific time and frequency of each patient interaction (e.g. specific information of when a patient logs-in and logs-out of an online patient portal, requests an appointment, or seeks information about a specific doctor, condition, treatment, or prescription drug), and the content of communications that patients exchange with their Health Care Providers, e.g., communications relating to specific medical issues.

2. Google's Conduct Is Unlawful and Individuals Have a Reasonable Expectation of Privacy Under State Laws

246. Google's unlawful acquisition and use of Health Information for which an individual has a reasonable expectation of privacy is well supported by state law. Indeed, nearly every state has recognized the highly personal and sensitive nature of Health Information such that specific laws have been enacted to protect this information.

247. Because the Google Terms of Service expressly adopts California law, Plaintiffs provide an overview of California law.⁹²

248. In California, the Health Information at issue is protected by, among other statutes and regulations, the California Invasion of Privacy Act, CMIA, CCPA, and California Civ. Code § 1798.91.

249. California Invasion of Privacy Act ("CIPA"): As with the ECPA, California's analog to the federal wiretap statute recognizes individuals' reasonable expectations of privacy that a third-party company like Google will not acquire the contents of their Health Information.

⁹² See Ex. 41, *Terms of Service*, GOOGLE PRIVACY & TERMS, at 12 (Jan. 5, 2022), <https://policies.google.com/terms> (asserting that "California law will govern all disputes arising out of or relating to these terms, service-specific additional terms, or any related services, regardless of conflict of laws rules"). The most recent Terms of Service for United States users states that it is effective as of January 2022. Citations to Google's Terms of Service herein are to the January 2022 version, attached hereto as Exhibit 41.

250. The CIPA provides similar prohibitions to the interception, acquisition, and/or use of the “content” of electronic communications, i.e. the substance, purport, or meaning of an electronic communication, without lawful consent of all parties to the communication. Cal. Penal Code § 631. As explained above, the Health Information at issue in this action pertains to the substance, purport or meaning of patient’s electronic health communications.

251. CMIA: The CMIA recognizes the inherently private and confidential nature of “medical information” and prohibits Health Care Providers from disclosing that information without first receiving valid written authorization from the patient. *See* Cal. Civ. Code § 56.10. The authorization required is heavily regulated and must, among other things, include specific uses and limitations on the type of medical information to be disclosed and provide an end date for the authorization. *See* Cal. Civ. Code §§ 56.11, 56.21. The CMIA also protects medical privacy by prohibiting entities other than licensed healthcare professionals from knowingly or willfully obtaining, disclosing, or using medical information without authorization. The CMIA imposes fines and civil penalties for such conduct, which are heightened when the medical information is used for “financial gain.” Cal. Civ. Code §§ 56.36(c)(2)-(3); 56.36(c)(5).

252. Under the CMIA, “medical information” is “any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient’s medical history, mental or physical condition, or treatment.” Cal. Civ. Code § 56.05(i). “[I]ndividually identifiable information” means that “the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient’s name, address, electronic mail address, telephone number, or social security number, or other information that reveals the individual’s identity.” *Id.*

253. The CMIA’s definition of medical information applies to the Health Information at issue here. Further, the CMIA supports the conclusion that California law recognizes individuals’ reasonable expectations of privacy over this information and that Google’s acquisition and use of patients’ Health Information is subject to the CMIA’s provisions regarding valid authorization.

254. CCPA: The CCPA recognizes and secures individuals' rights to privacy and control over the "personal information" that businesses may collect about them online. *See* Cal. Civ. Code § 1798.100. Violation of the CCPA may lead to civil actions and monetary damages. Cal. Civ. Code § 1798.150(a)(1).

255. The CCPA's definition of "personal information" includes:

a. "[I]nformation that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Cal. Civ. Code § 1798.140(v)(1). This includes any unique personal identifier, online identifier, Internet Protocol address, email address, account name, or other similar identifiers if they identify, relate to, describe, are reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household. *See* Cal. Civ. Code § 1798.140(v)(1)(A)-(C).

b. The CCPA identifies a sub-category of personal information as "sensitive personal information," and defines this to include "personal information collected and analyzed concerning a consumer's health." Cal. Civ. Code § 1798.140(ae)(2)(B).

256. Under the CCPA, a business that controls the collection of sensitive personal information (e.g. health-related information) shall, at or before the point of collection, inform consumers of the categories of sensitive personal information to be collected and the purposes for which the categories of sensitive personal information are collected or used, and whether that information is sold or shared. *See* Cal. Civ. Code § 1798.100(a)(2). A business shall not collect additional categories of sensitive personal information or use sensitive personal information collected for additional purposes that are incompatible with the disclosed purpose for which the sensitive personal information was collected without providing the consumer with notice consistent with this section. *See id.*

257. The CCPA's definition of personal information encompasses the Health Information at issue here. Further, the CCPA supports the conclusion that California law recognizes individuals' reasonable expectations of privacy over this information and that Google's acquisition and use of patients' Health Information is subject to the CCPA's provisions regarding valid disclosure.

258. California Civ. Code § 1798.91: Under Section 1798.91, a business may not request medical information directly from an individual – regardless of whether the information pertains to the individual or not – and use, share, or otherwise disclose that information for direct marketing purposes, without doing the following prior to obtaining that information:

- (1) Disclosing in a clear and conspicuous manner that it is obtaining the information to market or advertise products, goods, or services to the individual; and
- (2) Obtaining the written consent of either the individual to whom the information pertains or a person legally authorized to consent for the individual, to permit his or her medical information to be used or shared to market or advertise products, goods, or services to the individual.

See Cal. Civ. Code § 1798.91(c).

259. Under Section 1798.91, "direct marketing purposes" means "the use of personal information for marketing or advertising products, goods, or services directly to individuals." Cal. Civ. Code § 1798.91(a)(1).

260. Under Section 1798.91, "medical information" is defined in the same manner as used under the CMIA. *See Cal. Civ. Code § 1798.91(a)(2).*

261. Section 1798.91's definition of medical information encompasses the Health Information at issue here. Further, in order to obtain lawful consent for the conduct alleged herein, which includes the interception, acquisition and use of Health Information for purposes of targeted advertising, Google was required to comply with the provisions Section 1798.91 and it failed to do so.

262. Google's contracts and public statements with consumers expressly adopt California law to govern its relationship with consumers and Google's headquarters, decision-

making, and a substantial portion of the conduct alleged herein occurred in California. Thus, California law protects all Class Members.

263. However, to the extent Google argues, and the Court ever finds, to the contrary, every state in the country has civil and/or criminal laws that protect their citizens' privacy and property rights in their Health Information, communications content, and personal property—including their computing devices. In such an event, Plaintiffs reserve the right to amend to allege and add claims for violations of the various applicable laws of all 50 states.

3. Google's Conduct Is Unlawful and Individuals Have a Reasonable Expectation of Privacy Under Common Law

264. Google's unlawful acquisition of, and individuals' reasonable expectations of privacy over, their Health Information is well supported by common law, which has long protected the privacy and confidentiality of Health Information and communications. Among others, applicable common laws include:

a. Common Law Privacy Torts: Privacy torts, such as intrusion upon seclusion, public disclosure of private facts, and breach of fiduciary duty create a reasonable expectation that individuals' Health Information will not be shared without their knowledge or authorization, and that a third-party company will not obtain such information without their knowledge or authorization.

b. Property and Trespass: At common law, individuals have the right to possess, use, enjoy or dispose of their own property, and to exclude others from doing so without their authorization. This includes tangible property such as the computing devices that Google trespassed upon by placing Google Cookies causing the devices to redirect Health Information to Google. It also includes intangible property such as individuals' Health Information itself. *See, e.g. Fields v. Michael*, 91 Cal. App. 2d 443, 449 (1949) ("[t]he word 'property' may be properly used to signify any valuable right or interest protected by law"); *People v. Kozlowski*, 96 Cal. App. 4th 853 (2002) ("[t]he term [property] is all-embracing, including every

intangible benefit and prerogative susceptible of possession or disposition”); *People v. Kwok*, 75 Cal. App. 4th 1236, 1251 (1998) (property includes a copy of a key that is made without the owner’s knowledge when the original is returned to the owner, “which is analogous to making … an unauthorized copy of computer data”).

265. Accordingly, Google’s unauthorized interception, acquisition and use of patients’ Health Information, which is the private property of individuals, is actionable, both because of how Google obtained the information (by intermeddling with private personal property and converting it to a surveillance device) and because the information Google obtained through these methods *is* private property. Indeed, if Google broke into individuals’ homes, or a Health Care Provider’s brick-and-mortar facility, to steal the Health Information at issue here, there would be no doubt that would comprise an invasion of privacy and loss of property. Plaintiffs’ rights in this case are not any less worthy of legal protection.

I. Google’s Conduct Violates Its Own Express Promises

266. In addition to violating federal, state and common laws, Google’s misconduct also contravenes its own express promises.

267. As detailed below, Google’s Terms of Service and policy documents contain promises that Google will ensure compliance with applicable laws, that it will respect and protect privacy rights, that it will not collect Health Information without individuals’ consent, that it will not use Health Information for purposes of personalized advertising, and that it will use information obtained from other websites and applications to enforce, rather than to violate, these promises.

268. With respect to all patients, the promises reinforce patients’ expectations of privacy over their Health Information.

269. With respect to patients who are Google Account Holders, the promises operate as contractually binding terms between Google and Google Account Holders because Google

requires that all Google Account Holders expressly agree to these contracts of adhesion upon signing up to be a Google Account Holder.

270. With respect to patients who are non-Google Account Holders, i.e., those that were not required to expressly agree to the Google Terms of Service or policy documents, the documents nonetheless provide a basis for implied contract as Google maintains that these terms apply when anyone “interact[s] with [Google] services.”⁹³

1. The Google Terms of Service

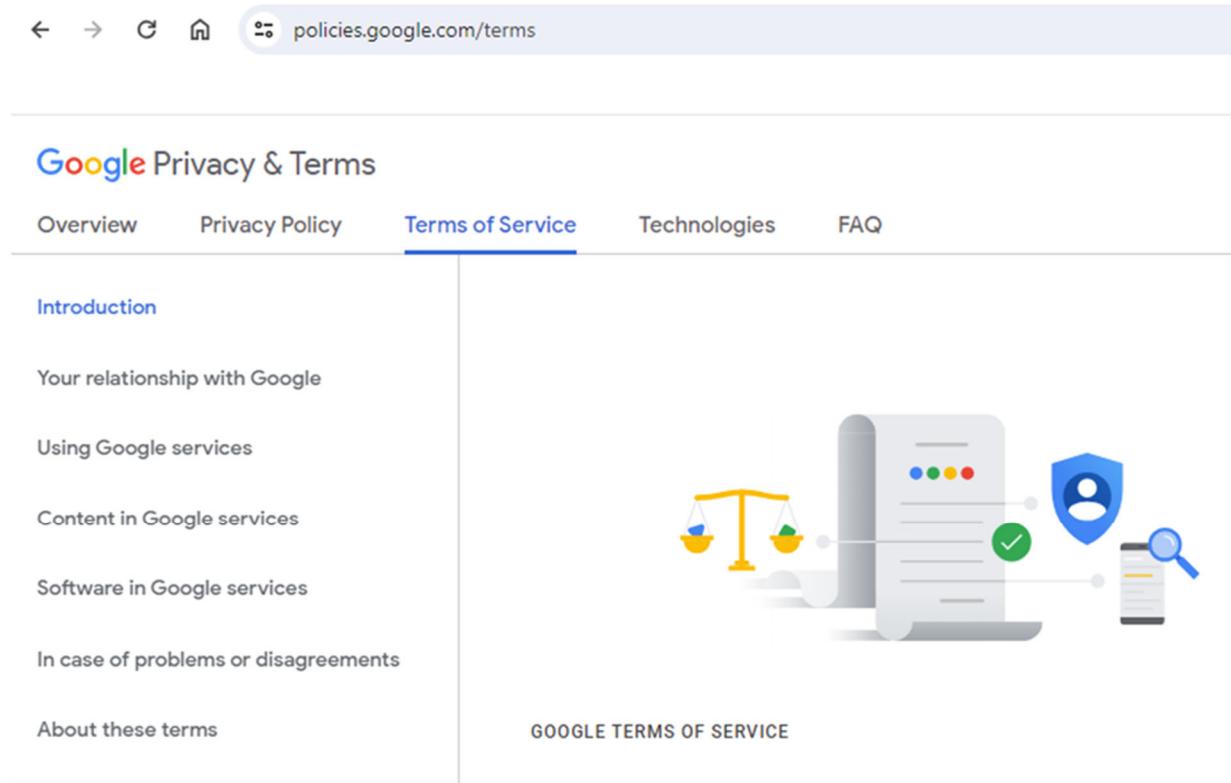
271. The Google Terms of Service states that it “establish[es] what you can expect from [Google] as you use Google services, and what [Google] expect[s] from you.” Google expressly identifies its Terms of Service document as a contract between Google and users, declaring that “by using our services, you’re agreeing to these terms . . .” and “you’re contracting with: Google LLC.”⁹⁴

272. Exhibit 41 cited herein is a downloadable PDF version of Google’s Terms of Service effective January 5, 2022. Google makes the PDF available on its website, but does not require that the PDF be downloaded or viewed to be binding. Instead, Google presents its Terms of Service to users as one of five webpages at the URL <https://policies.google.com/terms>. This URL is accessible via a “Terms” hyperlink at the bottom of numerous Google webpages, including the webpage to create a Google Account, to sign in, and to manage an account after logging in.

⁹³ See *id.* (Ex. 41) at 1.

⁹⁴ *Id.* (Ex. 41) at 1-2 (stating “these Terms of Service help define Google’s relationship with you as you interact with our services” (emphasis added) and that “by using our services, you’re agreeing to these terms”).

These five webpages, titled: “Overview,” “Privacy Policy,” “Terms of Service,” “Technologies,” and “FAQ,” are nested within a broader “Google Privacy & Terms” website, as follows:



The screenshot shows a web browser with the URL policies.google.com/terms in the address bar. The page title is "Google Privacy & Terms". A navigation bar at the top includes links for "Overview", "Privacy Policy", "Terms of Service" (which is underlined in blue), "Technologies", and "FAQ". On the left, a sidebar lists links: "Introduction", "Your relationship with Google", "Using Google services", "Content in Google services", "Software in Google services", "In case of problems or disagreements", and "About these terms". The main content area features a graphic with a balance scale, a document with a checkmark, a shield with a person icon, and a smartphone with a magnifying glass. The text "GOOGLE TERMS OF SERVICE" is centered below the graphic.

273. The tab titled “Overview” links to the “Privacy & Terms” Overview main page, which displays a menu bar in the upper left-hand corner with the same five menu options. The “Privacy Policy” menu option links to Google’s Privacy Policy webpage at the URL <https://policies.google.com/privacy>, containing additional hyperlinked menu options.⁹⁵ The “Terms of Service” menu option links to the Terms of Service webpage at the URL <https://policies.google.com/terms>, containing additional hyperlinked menu options. The “Technologies” menu option links to Google’s Policies Site/Technologies webpage at the URL <https://policies.google.com/technologies>, containing one paragraph of text and under the heading

⁹⁵ Google has changed the text in its Privacy Policy twice since this action was filed in May 2023, on July 1, 2023 and October 4, 2023. Plaintiffs refer herein to the version of Google’s Privacy Policy effective December 2022, which was in effect at the time this action was filed. A downloadable PDF copy of the December 2022 version of Google’s Privacy Policy is attached as Exhibit 42. As with the Terms of Service, Google imposes no requirement that users review the downloadable PDF version of its Privacy Policy.

“Technologies,” and additional hyperlinked menu options, including one for “Advertising.” The “FAQ” menu option links to Google’s Frequently asked Questions webpage at the URL <https://policies.google.com/faq>, containing additional hyperlinks.

274. On the Privacy & Terms Overview page, Google describes and presents hyperlinks to four other webpages, in addition to the five that are displayed via the five menu options. These include a hyperlink to the “Google Product Privacy Guide,” which Google states contains information about users’ “power to control and protect your personal information.”⁹⁶ In the Privacy Guide, Google presents numerous additional hyperlinks to information regarding Google Analytics and other Google Source Code, including the Google Analytics Help page for “Safeguarding Google Analytics Data” at the URL <https://support.google.com/analytics/answer/6004245>.⁹⁷

275. Google’s Terms of Service do not purport to exclude additional Google policies and terms from the scope of each user’s contractual agreement with Google. On the contrary, they state that “these Terms of Service *help* define Google’s relationship with you,” which, like Google’s presentation of the Terms of Service as one of numerous policy documents, indicates that the Terms of Service do not exclusively define the contractual relationship.⁹⁸ The Google Terms of Service webpage, like the Privacy & Terms Overview website of which it is a part, refers to and incorporates a large number of other Google-authored webpages.

276. For example, the Google Terms of Service declare that Google’s “service-specific additional terms and policies provide additional details about appropriate conduct that everyone using those services must follow,” where the underlined text links to a webpage titled “List of Services & Service-Specific Additional Terms.” On that hyperlinked “Additional Terms” webpage, Google clarifies that “[t]he Terms of Service, additional terms, and policies [i.e., not just

⁹⁶ See Ex. 43 (print-friendly reproduction of the “Overview” webpage <https://policies.google.com>) at 2.

⁹⁷ See Ex. 44 (partial screenshot of Google Product Privacy Guide URL, showing “Google Analytics” entries, at <https://policies.google.com/technologies/product-privacy>).

⁹⁸ Ex. 41, *supra* n.92 at 1 (emphasis added).

the Terms of Service or any “terms” as opposed to “policies” in isolation] define our relationship and mutual expectations as you use these services.” The Additional Terms webpage lists a number of Google products and directs the reader to more than 50 additional webpages via hyperlinks.⁹⁹ The Additional Terms webpage does not state that the hyperlinks identified thereon are the only additional terms and policies that form part of Google’s contract with users of Google products and services.

277. The Google Terms of Service also expressly incorporate the Google Privacy Policy webpage, and the Technologies/Policies Site webpage, declaring, “You also agree that our Privacy Policy applies to your use of our services. Additionally, we provide resources like the Copyright Help Center, Safety Center, and descriptions of our technologies from our policies site to answer common questions and to set expectations about using our services,” where the underlined “Privacy Policy” text hyperlinks to the same Privacy Policy webpage, and the underlined “policies site” text hyperlinks to the same Technologies/Policies Site webpage, that are accessible from the hyperlinks surrounding the nested Terms of Service and the Privacy & Terms Overview webpage main menu.¹⁰⁰

278. All of the information Google presents to users on the Privacy & Terms website is the same for all users, and not unique to a given individual or entity. The “you” used throughout Google’s Terms of Service and policies includes “business users and organizations,” not just the individual reading Google’s policies at a given point in time, as indicated by portions of the Google Terms of Service directed to and intended “[f]or business users and organizations only,” as well as Google’s introductory statement in its Terms of Service that they cover “what to expect in case someone violates these terms.”¹⁰¹ The contents of these policies are drafted exclusively by Google. Google presents these terms online, in an interactive format, with the full scope of information

⁹⁹ See generally Ex. 45, *List of Services & Specific Additional Terms*, GOOGLE PRIVACY & TERMS, <https://policies.google.com/terms/service-specific>.

¹⁰⁰ Ex. 41, *supra* n.92 at 4, and hyperlinks therein.

¹⁰¹ *Id.* (Ex. 41) at 1, 11.

viewable only via a complex web of hyperlinks, as a set of rules, principles, responsibilities, promises, and controls which Google itself agrees to respect, and to which all users of Google products and services must agree without alteration, in order for Google to permit their use of Google products and services.

2. The Express Promises in Google Policy Documents

279. Within the interconnected web of Policies and Terms that form the contract between Google and users of Google products and services, Google makes at least five promises that it has violated through its conduct alleged herein. By way of overview: Google promises to enforce rules of conduct for Google and all users of Google products and services by terminating uses that do not comply with the rules of conduct. The rules of conduct include prohibitions on using Google services to violate privacy laws, to disrespect others' rights, and to mislead or abuse other users. Specific promises by Google about the rules as applied to Health Information, and specific promises regarding Google's agreement to enforce and abide by these rules of conduct, are located in numerous Privacy & Terms documents that Google presents to users, including those attached hereto as Exhibits 41-51. The specific placement, incorporation into Google's contract with users, and contents of these Promises are described in more detail below.

280. Promise 1: Google's Terms of Service webpage is the first nested webpage to which Google directs the users of its products and services "to establish what you can expect from us as you use Google services, and what we expect from you."¹⁰² The Terms of Service webpage states that Google "want[s] to maintain a respectful environment for everyone," such that "you," i.e., any individual using Google products and services, "must follow these basic rules of conduct: comply with applicable laws . . . respect the rights of others, including privacy and intellectual property rights . . . [and] don't abuse or harm others or yourself (or threaten or encourage such abuse or harm) — for example, by misleading [or] defrauding . . . others."¹⁰³ Immediately below the rules

¹⁰² *Id.* (Ex. 41) at 1.

¹⁰³ *Id.* (Ex. 41) at 4.

that Google asserts it has created for Google services, consistent with the introductory statement that the Terms of Service tell users “what to expect in case someone violates these terms,” Google agrees to take responsibility for enforcing the rules of conduct, and advises that Google users may assist in those efforts: “If you find that others aren’t following these rules, many of our services allow you to report abuse,” where the “report abuse” text hyperlinks to a “Google Help” webpage in which Google declares that “[a]fter you submit a report, we’ll investigate it and take the appropriate action.”¹⁰⁴ The Terms of Service further confirm that Google promises to enforce its rules of conduct in declaring that “we [Google] give you [any user] permission to use our services if you agree to follow these terms,” indicating that Google agrees to withdraw its “permission” if any given user (“someone”) fails to follow the rules of conduct. Further below in the Terms of Service, Google again confirms that it has “the right to suspend or terminate your access to the services” if “you materially or repeatedly breach these terms [or] service-specific additional terms or policies,” or if “your conduct causes harm or liability [defined in a pop-up window to include ‘[l]osses from any type of legal claim’] to a user, third party, or Google — for example, by . . . , misleading others, or scraping content that doesn’t belong to you.”¹⁰⁵ Google further clarifies that “[i]f you [again, including organizations, businesses, and other users] don’t follow these terms or the service-specific additional terms, and we don’t take action right away, that doesn’t mean we’re giving up any rights that we may have, such as taking action in the future,” and “[i]f you don’t agree to the new terms, you should remove your content and stop using the services.”¹⁰⁶

281. Google repeats and reinforces its promise to enforce the rules of conduct on several of the policy webpages that are presented with its Terms of Service and incorporated therein, making additional specific promises consistent with its contractual responsibilities and agreed enforcement obligations.

¹⁰⁴ *Id.* (Ex. 41) at 1; Ex. 46, *Report Abuse or Legal Issue*, GOOGLE GROUPS HELP, <https://support.google.com/groups/answer/81275>.

¹⁰⁵ *Id.* (Ex. 41) at 1, 2, 12, 14-15.

¹⁰⁶ *Id.* (Ex. 41) at 13.

282. Promise 2: Google promises that Google does not collect Health Information that individuals do not choose to provide to Google. Under the sub-heading “Categories of information we collect,” the Google Privacy Policy identifies “health information” as a distinct category of information, and explains that Google’s collection of this information is limited to only when a person “choose[s] to provide it”: “Health information *if you choose to provide it*, such as your medical history, vital signs and health metrics (like blood glucose levels), and other similar information related to your physical or mental health, in the course of using Google services that offer health-related features, such as the Google Health Studies app.”¹⁰⁷

283. Promise 3: Google promises to enforce its rules of conduct regarding privacy rights, including for Health Information specifically. Under the heading “Why Google Collects Data,” in Google’s Privacy Policy, Google declares that Google does not show “personalized ads based on sensitive categories,” such as . . . health, where the underlined text expands to declare: “When showing you personalized ads, . . . [w]e don’t use topics or show personalized ads based on sensitive categories like race, religion, sexual orientation, or health. And we require the same from advertisers that use our services.”¹⁰⁸ The hyperlinked text “require the same from advertisers” links to Google’s “Advertising Policies Help” webpage, at the URL <https://support.google.com/adspolicy/answer/143465>.

284. Similar to Google’s nested presentation of Google’s Terms of Service as one of five menu options, the Advertising Policies Help webpage contains four tabs along the top, each of which, if clicked, reveals a different portion of the webpage. The “List of ad policies” tab is selected by default at the hyperlink from Google’s Privacy Policy, and the “Personalized advertising” policy,¹⁰⁹ one of several policy documents available under that menu option, is displayed. This page contains a description of advertising policies, numerous additional

¹⁰⁷ Ex. 42, *supra* n.95 at 17-18 (emphasis added).

¹⁰⁸ *Id.* (Ex. 42) at 5-6, 30 (underline/hyperlink original).

¹⁰⁹ Ex. 47, *Personalized Advertising*, GOOGLE ADVERTISING POLICIES HELP, <https://support.google.com/adspolicy/answer/143465>.

hyperlinks, and a list of other hyperlinked policies on its right-hand side. Google repeats and expands upon its promises to enforce the rules of conduct in the Personalized advertising policy, where Google promises that it prohibits advertising based on: “Restricted drug terms,” such as “prescription medications and information about prescription medications . . .;” and “personal health content,” such as “physical or mental health conditions, including diseases, sexual health, and chronic health conditions”; “[p]roducts, services, or procedures to treat or manage chronic health conditions...”; “any health issues associated with intimate body parts or functions...”; “invasive medical procedures”; and, “[d]isabilities, even when content is oriented toward the user’s primary caretaker,” and again confirms that “We don’t allow targeting users based on legally restricted content.”¹¹⁰

285. Google’s Personalized advertising policy also states that “Google’s privacy policy applies to all Google features and dictates how Google collects, uses, and protects user data. Learn about what happens if you violate our policies,” where the underlined text hyperlinks to another portion of the Advertising Policies Help webpage that is also accessible by selecting the “Review process” tab at the top and navigating to “Disapprovals and suspensions,” and selecting “What happens if you violate our policies.”¹¹¹ There, Google declares that “Google requires that advertisers comply with all applicable laws and regulations in addition to the Google Ads policies. Ads, assets, destinations, and other content that violate these policies can be blocked on the Google Ads platform and associated networks.”¹¹² Google goes on to promise that it will take corrective and punitive actions against advertisers and publishers that do not comply, including immediate suspension for egregious violations, which, in turn, is defined to include unlawful activity.¹¹³

¹¹⁰ *Id.* (Ex. 47) at 4, 5, 8.

¹¹¹ *Id.* (Ex. 47) at 1.

¹¹² Ex. 48, *What Happens if You Violate Our Policies*, GOOGLE ADVERTISING POLICIES HELP, at 1, <https://support.google.com/adspolicy/answer/7187501>.

¹¹³ *Id.* (Ex. 48) at 1-2.

286. In one of more than thirty additional hyperlinked policies listed to the right-hand side of the List of ad policies/Personalized advertising policy webpage, titled “Legal Requirements” Google confirms both the applicability of its rules of conduct to Health Information, and Google’s agreement to take responsibility for enforcement: “We expect all advertisers to comply with the local laws for any area their ads target, in addition to the standard Google Ads policies. We generally err on the side of caution in applying this policy because we don’t want to allow content of questionable legality.”¹¹⁴

287. Similarly, the Google Analytics “Safeguarding your Data” Help page that is made available via hyperlink from Google’s Product Privacy Guide on its Privacy & Terms Overview page (at the URL <https://support.google.com/analytics/answer/6004245>) is also hyperlinked from Google’s Privacy Policy within a discussion of Google Analytics, as follows: “[A]n advertiser may want to use its Google Analytics data to create more relevant ads, or to further analyze its traffic. Learn more,” where the text “Learn more” also directs users to the Safeguarding your Data webpage.¹¹⁵ On the Safeguarding your Data webpage, Google again makes and reaffirms its commitment to enforce the rules of conduct against privacy violations: “Laws protecting user privacy such as the European Economic Area’s General Data Protection Regulation and other privacy laws that establish various rights for applicable US-state residents impact content publishers, application developers, website visitors, and application users.... Google is committed to protecting data confidentiality and security.”¹¹⁶

288. Promise 4: Google promises to use the data it obtains from third-party websites and apps to help fulfill its agreement to enforce, rather than to violate, the rules of conduct.

¹¹⁴ Ex. 49, *Legal Requirements*, GOOGLE ADVERTISING POLICIES HELP, at 1 (Mar. 6, 2023). Google amended the language on this webpage after this action was filed. The webpage as it appeared in March 2023 is appended as Exhibit 49 hereto, and available at <https://web.archive.org/web/20230306142755/https://support.google.com/adspolicy/answer/6023676>.

¹¹⁵ Ex. 42, *supra* n.95 at 28.

¹¹⁶ Ex. 50, *Safeguarding Your Data*, GOOGLE ANALYTICS HELP, at 1, <https://support.google.com/analytics/answer/600424>.

Specifically, the Google Privacy Policy contains the text “Learn more about how Google uses data when you use our partners’ sites or apps,” where the text “Learn more” hyperlinks to the same Technologies/Policies Site webpage incorporated in and presented with the Terms of Service.¹¹⁷ The “Advertising” menu option and, within that, the “How Google uses information from sites or apps that use our services” option, are selected by default. This webpage is also hyperlinked from numerous other locations in Google’s Privacy Policy including one titled “Go to How Google uses information from sites or apps that use our services.”¹¹⁸ This portion of Google’s Technologies/Policies Site page explains that Google agrees to use the data it receives from third-party websites, such as Health Care Provider websites, to enforce its rules of conduct: “Google uses the information shared by sites and apps to … protect against fraud and abuse[.]”¹¹⁹

289. In sum, Google’s Privacy & Terms, Terms of Service, Privacy Policy and incorporated policy documents contain the following promises, illustrated with excerpts (bold-underline emphasis added), including hyperlinks, from Google’s contract documents as follows:¹²⁰

PROMISE 1

Google has established and enforces rules of conduct that prohibit violating laws and privacy rights through use of Google services.

These terms help define the relationship between you and Google. Broadly speaking, we give you permission to use our services if you agree to follow these terms, which reflect how Google’s business works and how we earn money. When we speak of “Google,” “we,” “us,” and “our,” we mean Google LLC and its affiliates.

....

We want to maintain a respectful environment for everyone, which means you must follow these **basic rules of conduct:**

- comply with applicable laws, . . .

¹¹⁷ Ex. 42, *supra* n.95 at 33.

¹¹⁸ *Id.* (Ex. 42) at 9.

¹¹⁹ Ex. 51, *Technologies: Advertising: How Google uses information from sites or apps that use our services*, GOOGLE PRIVACY & TERMS, <https://policies.google.com/technologies/partner-sites>.

¹²⁰ To the extent Google claims any other statement in a policy creates express or implied consent to the conduct at issue, any such consent is negated by, among other things, the express promises set forth above and the underlying reasonable expectation that Google will not participate in unlawful conduct.

- respect the rights of others, including privacy and intellectual property rights
- don't abuse or harm others or yourself (or threaten or encourage such abuse or harm) — for example, by misleading, [or] defrauding . . . others
- don't abuse, harm, interfere with, or disrupt the services — for example, by accessing or using them in fraudulent or deceptive ways, . . . or bypassing our systems or protective measures.

Our [service-specific additional terms and policies](#) provide additional details about appropriate **conduct that everyone using those services must follow**. If you find that others aren't following these rules, many of our services allow you to [report abuse](#). If we act on a report of abuse, we also provide the process described in the [Taking action in case of problems](#) section.

[report abuse](#): “After you submit a report, **we'll investigate it and take the appropriate action.**”

....

Google reserves the right to **suspend or terminate your access to the services** or delete your Google Account if any of these things happen:

- you materially or repeatedly breach these terms, [service-specific additional terms or policies](#)
- we're required to do so to comply with a legal requirement or a court order
- your conduct causes harm or [liability](#) to a user, third party, or Google — for example, by hacking, phishing, harassing, spamming, misleading others, or scraping content that doesn't belong to you

[liability](#): “Losses from any type of legal claim, whether the claim is based on a contract, tort (including negligence), or other reason, and whether or not those losses could have been reasonably anticipated or foreseen.”

....

If you don't follow these terms or the [service-specific additional terms](#), and we don't take action right away, that doesn't mean we're giving up any rights that we may have, such as taking action in the future.

PROMISE 2

Google only collects health information that users choose to provide.

Categories of information we collect

....

Health information if you choose to provide it, such as your medical history, vital signs and health metrics (like blood glucose levels), and other similar information related to your physical or mental health, in the course of using Google services that offer health-related features, such as the [Google Health Studies app](#).

PROMISE 3

Google categorically does not use information pertaining to health for advertising or permit others to do so.

WHY GOOGLE COLLECTS DATA

...

You can control what information we use to show you ads by visiting your ad settings in [My Ad Center](#).

- **We don't show you personalized ads based on sensitive categories**, such as race, religion, sexual orientation, or **health**.

sensitive categories: "When showing you personalized ads, we use topics that we think might be of interest to you based on your activity. For example, you may see ads for things like "Cooking and Recipes" or "Air Travel." **We don't use topics or show personalized ads based on** sensitive categories like race, religion, sexual orientation, or **health. And we require the same from advertisers that use our services.**"

[**require the same from advertisers:**](#)

Legal restrictions

Ads must comply with all applicable laws and regulations for all of the locations where your ads are showing.

We don't allow targeting users based on legally restricted content, as defined in the following sensitive interest categories.

....

- Restricted drug terms in personalized advertising. Prescription medications and information about prescription medications, unless the medication and any listed ingredients are only intended for animal use and are not prone to human abuse or other misuse.
- Health in personalized advertising. Personal health content, which includes:
 - Physical or mental health conditions, including diseases, sexual health, and chronic health conditions, which are health conditions that require long-term care or management.
 - Products, services, or procedures to treat or manage chronic health conditions, which includes over-the-counter medications and medical devices.
 - Any health issues associated with intimate body parts or functions, which includes genital, bowel, or urinary health.
 - Invasive medical procedures, which includes cosmetic surgery.
 - Disabilities, even when content is oriented toward the user's primary caretaker.
 - Examples: Treatments for chronic health conditions like diabetes or arthritis, treatments for sexually transmitted diseases, counseling services for mental health issues like depression or anxiety, medical devices for sleep apnea like CPAP machines, over-the-counter medications for yeast infections, information about how to support your autistic child.

Google's [privacy policy](#) applies to all Google features and dictates how Google collects, uses, and protects user data. Learn about [what happens if you violate our policies](#).

what happens if you violate our policies:

What happens if you violate our policies

.... Google requires that advertisers comply with all [applicable laws and regulations](#) in addition to the [Google Ads policies](#). Ads, assets, destinations, and other content that violate these policies can be blocked on the Google Ads platform and associated networks. Below is a list of various [ways we enforce policies and laws](#).

.... **Accounts may be suspended** if we find violations of our policies or the Terms & Conditions.

If we detect an egregious violation, your account will be suspended immediately without prior warning. An egregious violation of the Google Ads policies is [a violation so serious that it is unlawful or](#) poses significant harm to our users . . . For repeat violations of a policy, we issue strikes to your Google ads account and penalties progressively increase with each subsequent strike leading up to account suspension. . . . Remarketing lists that don't follow the Personalized advertising policy may be disabled. . . . If we contact you to request information related to compliance, you're required to respond in a timely manner and swiftly take any corrective action needed to follow our policies.

Legal requirements

We expect all advertisers to comply with the local laws for any area their ads target, in addition to the standard Google Ads policies. **We generally err on the side of caution in applying this policy** because we don't want to allow content of questionable legality.

Safeguarding your data

Laws protecting user privacy such as the European Economic Area's General Data Protection Regulation and other privacy laws that establish various rights for applicable US-state residents impact content publishers, application developers, website visitors, and application users.

.... **Google is committed to protecting data confidentiality and security.**

PROMISE 4

Google uses the information it obtains from other websites and applications to enforce the rules of conduct.

your activity on other sites and apps

This activity might come from your use of Google services, like from syncing your account with Chrome or your visits to sites and apps that partner with Google. Many websites and apps partner with Google to improve their content and services. For example, a website might use our advertising services (like AdSense) or analytics tools (like Google Analytics), or it might embed other content (such as videos from YouTube). These services may share information about your activity with Google and, depending on your [account settings](#) and the products in use (for instance, when a partner uses Google Analytics in conjunction with our advertising services), this data may be associated with your personal information.

[Learn more](#) about how Google uses data when you use our partners' sites or apps.

Sites and apps that use Google services

Manage information that websites and apps using Google services, like Google Analytics, may share with Google when you visit or interact with their services.

[Go to How Google uses information from sites or apps that use our services](#)

[Learn more](#) and [Go to How Google uses information from sites or apps that use our services](#):

Google uses the information shared by sites and apps to deliver our services, maintain and improve them, develop new services, measure the effectiveness of advertising, [protect against fraud and abuse](#), and personalize content and ads you see on Google and on our partners' sites and apps.

3. Google Violates These Promises

290. Google violates each of the above promises because it does not protect users by enforcing or complying with the ostensible rules against violations of law, privacy, and/or misleading and fraudulent conduct. Google does, in fact: use Health Information to show ads based on sensitive categories, like health; does not prevent its advertisers from using and showing targeted ads based on sensitive categories, like health; permits targeting and advertising based on restricted drug terms and personal health content; and does not disable remarketing lists that fail to comply with Google's personalized advertising policy (i.e., prohibition on the use of showing of personalized ads based on sensitive categories). Google does not require Health Care Providers to comply with applicable law, to respect privacy rights, or to refrain from engaging in misleading or fraudulent conduct in the unlawful tracking, collection and disclosure to Google of patients'

Health Information, nor does it use its systems to prevent these abuses. Instead, the Google Source Code deposits Google Cookies on a patient's device that are disguised as first-party cookies and thus can, and do, track a given patient or browser across unrelated websites. Further, Google can and does link the Health Information collected, including the Health Information collected and redirected to Google Analytics, across its various systems and products to be used in its advertising services. Further, Google does not take action to stop, suspend, or discipline itself or a Health Care Provider for unlawful conduct (which under Google's own definition constitutes "egregious conduct") involving Google's collection of Health Information from Health Care Providers and it does not "err on the side caution" in enforcing these commitments but, instead, creates a system that facilitates the use and showing of targeted advertising based on sensitive categories, like health. Finally, Google shares personal Health Information with dozens of other companies, including for marketing purposes by those other companies and to aid those other companies in forming their own health-based profile information, through the Google Tag Manager source code.

291. Google publicly acknowledges that it does not keep its health advertising promises for its United States users.

292. On a page titled "Healthcare and medicines," Google provides advertisers with a list "of health care content that [Google] allow[s] in certain circumstances" for advertising.¹²¹

293. The "Healthcare and medicines" page for advertisers is not mentioned in the Google Terms of Service; Google Privacy Policy; or the body of the "Personalized advertising" help page.

294. Although Google prohibits the use of Health Information for advertising purposes in dozens of countries across a broad range of health categories, the United States is an exception.

¹²¹ Ex. 52, *Healthcare and Medicines*, GOOGLE ADVERTISING POLICIES HELP (archived), at 1, <https://web.archive.org/web/20230203100832/https://support.google.com/adspolicy/answer/176031>.

295. For example, Google does not permit advertising for prescription drug manufacturers in Europe, but does in the United States:¹²²

Pharmaceutical manufacturers

Google allows pharmaceutical manufacturers to advertise in select countries only.

Prescription drugs

Pharmaceutical manufacturers may promote prescription drugs in the following countries only: Canada, New Zealand, United States. Pharmaceutical manufacturers may not promote prescription opioid painkillers.

Over-the-counter medicines

Pharmaceutical manufacturers may promote over-the-counter medicines in the following countries only: Australia, Austria, Brazil, Canada, China, Czech Republic, France, Germany, Hungary, Hong Kong, India, Italy, Japan, Kenya, Mexico, Netherlands, New Zealand, Norway, The Philippines, Poland, Portugal, Russia, Slovakia, South Korea, Spain, Sweden, United Kingdom, United States

Other manufacturers and suppliers

Bulk drug manufacturers, medical professional suppliers, and antibody/peptide/compound suppliers for commercial labs may advertise in the following countries only: Canada, United States

Certification

Pharmaceutical manufacturers must be certified by Google in order to serve ads. See [how to apply](#) below.

296. Google sets up a certification process to expressly permit health ads:¹²³

Apply for healthcare products and services certification

Certain advertisers — such as online pharmacies, pharmaceutical manufacturers, and others looking to use prescription drug terms in ad text or landing pages or health insurance advertisers in the United States — need to be certified with Google in order to advertise. If you are such an advertiser, here's how to apply to be certified:

1. Adhere to all country-specific requirements below. If your campaign targets a country that isn't listed, then we don't allow the promotion of prescription drugs or over-the-counter medicines by pharmaceutical manufacturers in that country.
2. Fill out our [online application form](#).
 - Please be sure to include your Google Ads customer ID, located at the top of your account pages.
 - To cut down on any unnecessary delays, be sure to fill out all of the requested information.
 - If you are an agency applying on behalf of an advertiser, please send documentation detailing your relationship with the advertiser or license holder.

¹²² *Id.* (Ex. 52) at 1-2.

¹²³ *Id.* (Ex. 52) at 18-19.

297. Google permits online pharmacies to target by Health Information:¹²⁴

Google restricts the promotion of online pharmacies. To determine whether an advertiser is promoting an online pharmacy, we consider a number of factors such as the content of your ads and site or app, as well as the products or services that you offer. For user safety and other reasons, we err on the side of caution in applying this policy, especially for landing pages that link or refer to content that in any way appears to be the online sale of medicines, whether prescription or over-the-counter medicine.

Countries

Google allows the promotion of online pharmacies in only these countries: Australia, Austria, Brazil, Canada, China, Czech Republic, Denmark, Germany, Hong Kong, Israel, Japan, Kenya, Mexico, Netherlands, New Zealand, Norway, Portugal, Russia, Slovakia, Sweden, Taiwan, United Kingdom, and the United States.

Google does not allow the promotion of online pharmacies in other countries.

Keywords

Google allows online pharmacy advertisers to bid on keywords containing prescription drug terms in only the following countries: Australia, Austria, Canada, Czechia, Denmark, Germany, Israel, Japan, Kenya, New Zealand, Netherlands, Norway, Portugal, Slovakia, United Kingdom, and United States.

Certification

Online pharmacies must be certified by Google in order to serve ads — see [how to apply](#) below. To be certified with Google, online pharmacies must be registered with the relevant pharmaceutical authorities in the countries that their ad campaign targets.

///

///

///

///

///

///

///

///

///

///

///

¹²⁴ *Id.* (Ex. 52) at 4.

298. Google permits the use of prescription drug terms for advertising:¹²⁵

In most parts of the world, Google doesn't allow the use of prescription drug terms in ad text, landing pages, keywords, or source code of a web page.

- For campaigns targeting Canada, New Zealand, or the United States, certain businesses such as online pharmacies and pharmaceutical manufacturers may use prescription drug terms in ad text and landing pages. While you do not need to be certified in order to serve your ads, you must be certified in order to keyword target prescription drug terms. These businesses must be certified by Google in order to serve ads — see [how to apply](#) below.
- If your campaigns do not target Canada, New Zealand, or the United States, you may not use prescription drug terms in ad text or landing pages.
- In limited cases, and where permitted by local law, Google allows exceptions to this policy for public health and safety awareness campaigns from governmental or well-established non-profit health advocacy organizations. If you would like to apply for such an exception to use prescription drug terms in ad text, landing pages, keywords, or source code of a web page, please [contact us](#).

See a non-exhaustive list of [prescription drugs](#) or active ingredients that are monitored under this policy.

299. Google “monitor[s]” at least 4,291 “prescription drugs … in Google Ads.”¹²⁶

300. Although prohibited elsewhere, Google tells advertisers that it permits advertising based on the following health-related items in the United States as long as the advertiser registers with Google:

- a. “Google only allows ads for addiction services in Australia, Ireland, New Zealand, and the United States. Google does not allow ads for addiction services in other countries. … Addiction services advertisers must be certified by Google in order to serve ads.”¹²⁷
- b. “Google prohibits the promotion of HIV home tests everywhere in the world except in the United States, France, the Netherlands, and the United Kingdom. In

¹²⁵ *Id.* (Ex. 52) at 5.

¹²⁶ A listing of “examples” of prescription drugs that Google monitors in Google Ads is available at *Prescription Drugs*, GOOGLE ADVERTISING POLICIES HELP, <https://support.google.com/adspolicy/answer/2430794>.

¹²⁷ Ex. 52, *supra* n.121 at 17.

the United States, advertisers may promote home HIV tests that are FDA approved.”¹²⁸

c. “Google does not allow the promotion of DHEA products anywhere except the United States[.]”¹²⁹

d. “Google does not allow the promotion of Melatonin products anywhere except Canada and the United States.”¹³⁰

e. Google allows ads for prescription opioid painkillers “intended for use as medication-assisted treatment (MAT) for opioid use disorder,” but only for: (a) public health and safety awareness campaigns from governmental or well-established non-profit health advocacy organizations; (b) ads for non-opioid pharmaceuticals that only refer to prescription opioids in their safety information; and (c) “certified addiction treatment providers in the United States. If you would like to apply for such an exception, please contact us.”¹³¹

f. Though prohibited in some countries, Google “allow[s] the promotion of clinical trial recruitment” in the United States.¹³²

g. Abortion and birth control.¹³³

h. “In the United States, you must be certified by Google in order to advertise health and medical insurance coverage, with the exception of government advertisers, who will be pre-approved. Advertisements exclusively for dental, vision, and/or travel health insurance coverage are not restricted. ... Health and

¹²⁸ *Id.* (Ex. 52) at 12.

¹²⁹ *Id.* (Ex. 52) at 7.

¹³⁰ *Id.* (Ex. 52) at 7.

¹³¹ *Id.* (Ex. 52) at 9.

¹³² *Id.* (Ex. 52) at 10-11.

¹³³ *Id.* (Ex. 52) at 13-16.

medical insurance providers ... must be certified by Google in order to serve ads in the United States.”¹³⁴

301. The “healthcare-related advertising” page starts with the following:¹³⁵

Apply for healthcare-related advertising

Please select what your organization is

- Online Pharmacy
- Pharmaceutical Manufacturer
- Governmental or well-established non-profit health advocacy organizations
- Addiction Services Provider
- Health Insurance Advertiser (Only for United States)
- Entity that holds an FDA-issued license or approval to market a cell or gene therapy (only for the United States)

302. Through this interface, Google is able to specifically identify all advertisers who it approves to serve health-care related advertising in these categories.

J. Google Acknowledges that Google Analytics Is Not Appropriate for Web Properties that Deal with Protected Health Information

303. Google publicly states that Google Analytics is not appropriate for web properties that implicate Health Information. In a web page titled, “HIPAA and Google Analytics,” Google cautions that Google Analytics results in data collection and thus web properties must ensure that they meet all applicable legal requirements. The full text of Google’s own warning is set forth below: ¹³⁶

¹³⁴ *Id.* (Ex. 52) at 17-18.

¹³⁵ See *Apply for Healthcare-Related Advertising*, GOOGLE ADS HELP, <https://support.google.com/google-ads/troubleshooter/6099627> (last visited Nov. 12, 2023).

¹³⁶ Ex. 1, *supra* n.5 at 1-2.

HIPAA and Google Analytics

Google Analytics is a measurement solution that can be used to obtain business insights about traffic on your websites and apps. It is important to ensure that your implementation of Google Analytics and the data collected about visitors to your properties satisfies all applicable legal requirements.

Please remember that to protect user privacy, Google Analytics policies and terms mandate that no data be passed to Google that Google could recognize as [personally identifiable information \(PII\)](#), and no data you collect using Google Analytics may reveal any sensitive information about a user, or identify them. If you need to delete data from the Analytics servers for any reason, you can schedule [a data-deletion request](#) or [use the User Deletion API](#).

What is HIPAA and to whom does it apply?

The [Health Insurance Portability and Accountability Act of 1996 \(HIPAA\)](#) is a US federal law that applies to HIPAA-regulated entities. The law and its implementing regulations typically are not relevant to Google Analytics customers operating exclusively outside of the US, nor are they relevant to every customer operating within the US. Analytics customers are responsible for determining whether they are HIPAA-regulated entities and what their obligations are under HIPAA.

Can Google Analytics be used in compliance with HIPAA?

Customers must refrain from using Google Analytics in any way that may create obligations under HIPAA for Google. HIPAA-regulated entities using Google Analytics must refrain from exposing to Google any data that may be considered Protected Health Information (PHI), even if not expressly described as PII in Google's contracts and policies. Google makes no representations that Google Analytics satisfies HIPAA requirements and does not offer Business Associate Agreements in connection with this service.

For HIPAA-regulated entities looking to determine how to configure Google Analytics on their properties, the [HHS bulletin](#) provides specific guidance on when data may and may not qualify as PHI. Here are some additional steps you should take to ensure your use of Google Analytics is permissible:

- Customers who are subject to HIPAA must not use Google Analytics in any way that implicates Google's access to, or collection of, PHI, and may only use Google Analytics on pages that are not HIPAA-covered.
- Authenticated pages are likely to be HIPAA-covered and customers should not set Google Analytics tags on those pages.
- Unauthenticated pages that are related to the provision of health care services, including as described in the HHS bulletin, are more likely to be HIPAA-covered, and customers should not set Google Analytics tags on HIPAA-covered pages..
- Please work with your legal team to identify pages on your site that do not relate to the provision of health care services, so that your configuration of Google Analytics does not result in the collection of PHI.

304. Although Google asks developers to “work with your legal team” to figure out how to use Google Analytics in a way that complies with HIPAA,¹³⁷ Google itself has the capability to make these determinations using its own systems.

305. As described above, Google has a crawler that scrapes and analyzes the content of every website and webpage that is scanned for inclusion in its search results. After analyzing each page, the Google crawler categorizes it and the content contained within it. For this purpose, Google maintains detailed content categorizations for websites and webpages, including categorizations related specifically to Health Information and Health Care Providers.

306. Despite making promises that Google will endeavor to prevent abuse of its systems, and that it will not collect or monetize Health Information, Google does not make use of its actual systems to prevent the collection of Health Information from Health Care Providers. Instead, Google permits and encourages Health Care Providers to use the same tools as any other advertiser or publisher to enable Google to collect Health Information—and to use such information for purposes of targeted advertising, including remarketing and targeting to health keywords on Google’s search engine, www.Google.com, on its Display Ad network, YouTube, and YouTube TV.

K. Google Has Not Obtained Consent from Healthcare Providers to Engage in the Specific Conduct Alleged

307. Google has denied engaging in the conduct alleged throughout this complaint. The fact that Google denies the conduct at issue negates any argument that it obtained actual consent from any Healthcare Provider for the conduct that Google publicly denies.

308. Google also cannot prevail on consent because the Google Privacy Policy, to which all publishers, advertisers, and consumers must agree to, make statements and promises that it will not collect, share or use Health Information.

¹³⁷ *Id.* (Ex. 1) at 2.

309. The Google Privacy Policy is expressly incorporated by hyperlinked reference for consumer accounts as well as publisher and advertiser accounts for Google Ads, Google Display Ads, Google Analytics, Google Ad Manager, YouTube, and Google APIs.

310. For example, when signing up for a Google Ad Manager account, Google states that, “Google’s use of your information will be in accordance with Google’s privacy policy.”¹³⁸ Further, when signed-in to their publisher or advertiser account, Google expressly incorporates a hyperlink to the Google Privacy Policy just beneath the account manager’s name in the “account information” box that it places in the top right corner of every screen when a publisher or advertiser is working within the Google tools at issue here.

311. In applying the Google Privacy Policy to all consumers, publishers, and advertisers, Google also applies the same promises set forth above to all such persons and entities.

312. In the Google Privacy Policy, Google expressly defines “personal information” broadly as “information that you provide to us which personally identifies you, such as your name, email address, or billing information, or other data that can be reasonably linked to such information by Google, such as information we associate with your Account.”¹³⁹

313. The Google Terms of Service expressly adopts California law,¹⁴⁰ which defines “personal information” in Cal. Civ. Code § 1798.140.

314. Google’s contracts with Healthcare Providers expressly assure Healthcare Providers or otherwise give those providers the impression that Google is (1) only collecting information where it has a person’s consent to do so; (2) not associating signed-in and signed-out activity; and (3) not collecting personally identifiable information through Google Source Code.

315. For Healthcare Providers that “Activate Google signals,” Google states: “When you choose to activate Google Signals, Google Analytics will associate the visitation information it

¹³⁸ See *Get started with Google Ad Manager*, GOOGLE AD MANAGER, <https://admanager.google.com/home/contact-us/> (last visited Nov. 13, 2023).

¹³⁹ Ex. 42, *supra* n.95 at 23.

¹⁴⁰ Ex. 41, *supra* n.92 at 12.

collects from your site and/or apps with Google information from accounts of signed-in users who have consented to this association for the purpose of ads personalization.”¹⁴¹

316. This purported Google Signals consent is limited and deficient in several respects.

317. *First*, it does not impact Google’s ability to collect Health Information, associate that information with users, or use that data for purposes other than ads personalization, such as to improve its ad targeting and attribution models or machine learning processes.

318. *Second*, Google expressly promises that it will only engage in such activity for “*users who have consented* to this association for the purpose of ads personalization.” However, as set forth herein, Plaintiffs and other patients in the putative class did not consent.

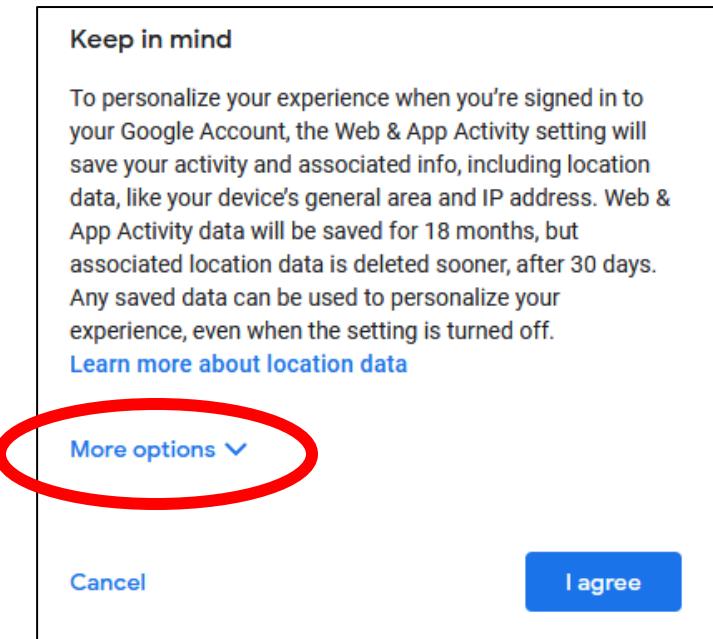
319. *Third*, Google’s statement is limited to its cross-analysis, use, and “association” of visitation information from “accounts of signed-in users.” Thus, to the extent it has obtained any consent at all, that consent is limited to “signed-in users.” However, as set forth herein, the Google Source Code surveils and co-mingles patient data regardless of whether they are “signed-in” or not. For example, Google associates Google Account ID information with Biscotti, Zwieback, ‘cid,’ YouTube Visitor ID, and many other identifiers and information that go well beyond any consent that can be found from this statement.

320. *Fourth*, even for web-properties unrelated to Health Information, Google’s process for obtaining purported “consent” to use information for purposes of “ads personalization” does not obtain actual consent. Instead, Google turns the “consent” control (called Google Ads Personalization) on by default and hides information about it from the consumer in the sign-up process. As set forth above, the Privacy and Terms contract of adhesion that Google imposes on consumers expressly promises users that, among other things, Google (1) will only collect “Health information if you choose to provide it,” and (2) Google “[w]on’t show you personalized ads based on sensitive categories, such as ... health.” Further, the Google Terms of Service states that “[t]he Google services that are subject” to the Terms are listed at

¹⁴¹ See ¶ 183, *supra*.

<https://policies.google.com/terms/service-specific>, a list that does not include Google Ads, Google Display Ads, Google Analytics, YouTube, or Google APIs. Rather, Google expressly states that YouTube has a separate terms of service and that Google’s “developer API products have their own terms as well.”¹⁴²

321. After more than two pages of text, the following appears at the bottom of the “Privacy and Terms” contract of adhesion shown to all Google Account Holders during sign-up:



|||||

¹⁴² Ex. 45, *supra* n.99, at 1.

322. If and only if a person clicks the “More option” link, an even longer set of text emerges. The first set of text is titled “Web & App Activity.” The second set of text relates to the purported “ads personalization” setting, and states:

Ad personalization

Google can show you ads based on your activity on Google services (such as Search or YouTube), and on websites and apps that partner with Google.

Show me personalized ads

Show me ads that aren't personalized

[Learn more about Ad personalization](#)

323. The “Show me personalized ads” button is checked-on by default – and remains on unless the person clicks the “Learn more” link, scrolls down to this text, and changes the default.

///

///

///

///

///

///

///

///

///

///

///

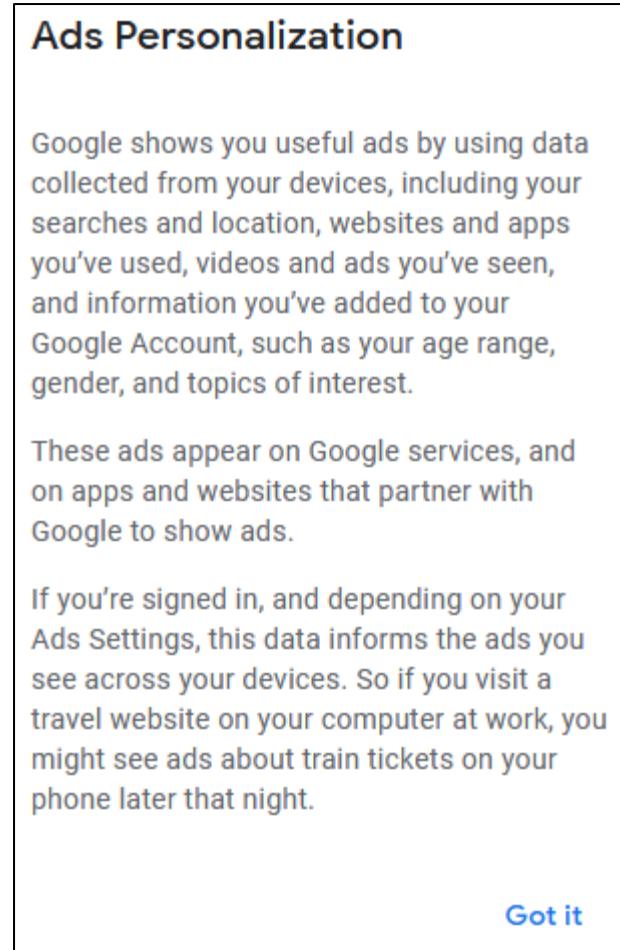
///

///

///

///

324. If a user clicks to “Learn more about Ad personalization,” the following appears:



325. To the extent that this may garner consent for anything, it does not garner consent to Google’s surveillance of Health Information on Health Care Provider properties because it does not refute the specific express promises that Google makes elsewhere regarding Health Information and how it may be used by Google.

326. In the next sentence of the “Activate Google signals” screen, Google states that the “Google information” that it associates with the “visitation information” “may include end user location, search history, YouTube history, and data from sites that partner with Google—and is used to provide aggregated and anonymized insights into your users’ cross device behaviors.”

327. The second sentence of the purported “Google Signals” consent is also limited and deficient in several ways.

328. *First*, Google does not tell publishers that Google connects the data to a person’s Google Account ID (i.e. their GAIA ID)—and the other information that Google associates with an Account ID, including name, email address, device identifiers, or signed-out identifiers. Thus, it does not provide consent for Google’s actual practice of linking the “visitation information,” including communications content to personally identifiable information.

329. *Second*, Google tells publishers activating Google signals that the data “is used to provide *aggregated and anonymized* insights into your users’ cross device behaviors.” However, as set forth herein, Google’s surveillance and use of the Health Information from Health Care Providers is neither aggregated nor anonymized but is rather particularized and identifiable. Even if what it presents to Health Care Providers appears anonymized to those Health Care Providers, it is actually identifiable to Google within Google’s systems.

330. Google also gives publishers (including Health Care Providers) the impression that Google Analytics does not collect personally identifiable information.

331. In the Google Analytics Terms of Service, another binding contract of adhesion (this time between Google and publishers using Google Analytics), Google requires, as a condition of using Google Analytics, that publishers “will not and will not assist or permit any third party to pass information, hashed or otherwise, to Google that Google could use or recognize as personally identifiable information, except where permitted by, and subject to, the policies or terms of Google Analytics features made available to you, and only if, any information passed to Google for such Google Analytics feature is hashed using industry standards.”¹⁴³

332. A reasonable reading of this provision is that Google Analytics is not automatically configured to collect personally identifiable information, but instead there are certain features that could be turned on if PII is hashed. However, contrary to the impression that Google gives, Google Analytics collects personally identifiable information by default.

¹⁴³ Dkt. 48-4, Google Analytics Terms of Service, Ex. 3 to Ganem Declaration at ¶ 7.

333. Other statements to publishers are even more explicit. In a document submitted by Google titled “Best practices to avoid sending Personally Identifiable Information (PII),” Google tells publishers that, “To protect user privacy, Google policies mandate that no data be passed to Google that Google could use or recognize as personally identifiable information (PII).”¹⁴⁴

334. Further down in the document submitted by Google, Google states:

The basic Analytics tag collects the page URL and page title of each page that is viewed. PII is often inadvertently sent in these URLs and titles. PII is often inadvertently sent in these URLs and titles. Both the URL path and parameters must be free of PII. If there is any possibility of your URLs, URL parameters, or titles containing PII, you’ll need to remove it.¹⁴⁵

However, unbeknownst to publishers, the “basic Analytics tag” is designed to, and does, automatically collect PII in the form of the “cid” data parameter that Google inserts into the page URL, and then connects to user identifiers, such as Biscotti that is linked to Gaia, Zwieback, device IDs, IP addresses, User-Agent information, geo-location, addresses, phone numbers, names, and other information in Google’s systems.

335. Google Analytics furthers the impression that it does not collect personally identifiable information through its marketing of an “IP address masking” feature in Analytics. In another document submitted by Google with the Ganem Declaration, Universal Google Analytics has a setting that “truncates” the IP address of a person “as soon as technically feasible” by removing the “last octet of IPv4 user IP addresses and the last 80 bits of IPv6” after they are “sent to Google Analytics and asserting that “[t]he full IP address is never written to disk” when the feature is turned on.¹⁴⁶ Beginning in December 2022, Google began transitioning all publishers

¹⁴⁴ Dkt. 48-6, Ganem Decl. Ex. 5 at 1.

¹⁴⁵ Google, Ganem Ex. 5 at 1.

¹⁴⁶ Google, Ganem Decl. Ex. 21, Dkt. 48-22 at 2.

from “Universal Analytics” to “Google Analytics 4,” where it states that “IP masking is not necessary since IP addresses are not logged or stored.”¹⁴⁷

336. However, for privacy purposes, Google Analytics’ IP address truncation (and even absence of collecting IP address at all) is a distinction without a difference because the information Google collects from Google Analytics is personally identifiable as a matter of fact and law even when the IP address is fully removed.

337. Google makes substantially similar statements to publishers regarding its other ads and marketing products. For Google Ad Manager, Google tells all publishers in its “Ad Manager and Ad Exchange program policies” that:

In the interests of protecting user privacy, Google ads product policies mandate that publishers must not pass any data to Google that Google could use or recognize as personally identifiable information (PII).¹⁴⁸

In a related statement titled “False Positive and Personally Identifiable Information,” Google tells publishers who have received a notification that they are sending PII what to do to either “fix the issue” or to identify whether there’s a “common false positive” situation.¹⁴⁹

338. To the extent that any Health Care Provider did consent—despite Google’s denials, promises, and statements to the contrary—any such consent is unlawful, criminal, and tortious in that it would be a knowing violation of patients’ reasonable expectations of privacy; common law privacy rights; federal health privacy and unfair business practice statutes; the laws of California and every state (including criminal and civil laws such as computer crime and unfair business statutes); trespass; conversion; and a common conspiracy with Google to violate the express privacy promises that Google makes to that Health Care Provider’s own patients.

¹⁴⁷ *Id.* As of July 1, 2023, Google announced that “standard Universal Analytics properties stopped processing data” and that “new data will only flow into Google Analytics 4 properties” after that date. Ex. 53, *Introducing the Next Generation of Analytics, Google Analytics 4*, GOOGLE ANALYTICS HELP, at 1, <https://support.google.com/analytics/answer/10089681>.

¹⁴⁸ Ex. 54, *Best Practices to Avoid Sending Personally Identifiable Information (PII)*, GOOGLE AD MANAGER HELP, at 1, <https://support.google.com/admanager/answer/6156630>.

¹⁴⁹ Ex. 55, *False Positives and Personally Identifiable Information (PII)*, GOOGLE AD MANAGER HELP, at 1, <https://support.google.com/admanager/answer/6157752>.

L. Internally, Google Executives Acknowledge It Does Not Obtain Actual Consent to Any of Its Surveillance, Much Less Health Surveillance

339. Google understands that it has not obtained actual consent.

340. In an internal study conducted by Google that included interviews of Google executives on the topic of consent, those executives candidly admitted that Google's consent model is broken. The interview notes from those executives include the following statements:

- a. "If people were the deciders, they wouldn't take the deal, but they are not the deciders."
- b. "[O]ur ads system as design[ed] doesn't really give the user choice."
- c. "We have gaps in how our system works and what we promise to people."
- d. "At Google, we still seem to believe in that fantasy that users agreed to this."
- e. "Consent is no longer consent if you think of ads as a product."
- f. "One example are all the controls that we have that have horrible names that don't mean anything to anyone, not even within the company."
- g. "When I look at UDC, what is sWAA v. WAA v. YT? They don't make sense ... and there are hidden functions that people don't know."
- h. There is "[n]o coherent and simple access to privacy controls across all apps, in Chrome and Android."
- i. "Everyone is concerned about their data being collected. They don't know about it and they don't know how to control it."
- j. The "[c]omplexity of the technology ... is beyond the grasp of nearly everyone ... We are transferring the onus of all that complexity from companies to users."
- k. "The fact that we can't explain what we have on you to users is probably our biggest challenge" on privacy. "I don't have the faintest idea what Google has on me."
- l. "Users have a right to know. The reasons we provide are so high level and abstract that they don't make sense to people."

- m. "I don't like the idea of [G]oogle having data about users that they can't say no to."
- n. "We know privacy is a core user need."
- o. "Users don't know what is happening under the hood."
- p. "[Users] don't understand what is going on[.] They need to be equal stakeholders. They don't understand what is going on."
- q. "Won't it creep people out to know how much we are paying attention."
- r. "Signup flows are not a good moment to explain or present these kinds of things to users."
- s. "We need to get to a degree of simplicity and honest[y] with the public and our users."¹⁵⁰

M. Patients' Health Information Has Actual and Measurable Monetary Value

341. The value of personal data, including the Health Information at issue in this case, is well understood and generally accepted as a form of currency.

342. Indeed, the existence of a robust market for personal data is well-recognized in news and academia.¹⁵¹ For example, a 2015 article from TechCrunch accurately noted: "Data has become a strategic asset that allows companies to acquire or maintain a competitive edge."¹⁵² Notably, the value of a single Internet user—or really, a single user's data—varied from about \$15

¹⁵⁰ See *Calhoun v. Google*, No. 4:20-cv-05146-YGR, Dkt. 910-2 at 12.

¹⁵¹ See, e.g., *The World's Most Valuable Resource is No Longer Oil, but Data*, THE ECONOMIST (May 6, 2017), <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> (comparing the digital market for user data to be analogous to the oil industry) (last visited Nov. 13, 2023); SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM, 166 (2019) (explaining that revenue from user data pervades every economic transaction in the modern economy); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2056-57 (2004) (noting "[p]ersonal information is an important currency in the new millennium" and that "[t]he monetary value of personal data is large and still growing....Companies view this information as a corporate asset and have invested heavily in software that facilitates the collection of consumer information").

¹⁵² Pauline Glickman and & Nicolas Gladys, *What's the Value of Your Data?*, TECHCRUNCH (Oct. 13, 2015), <https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/> (last visited Nov. 13, 2023).

to more than \$40; an interactive chart cited in the article demonstrates that each additional data point regarding particular health conditions adds to the value of a given user's information.¹⁵³

343. The Organization for Economic Cooperation and Development ("OECD"), an intergovernmental organization with 38 member countries (including the United States), has published numerous volumes discussing how to value data such as that which is the subject matter of this Complaint, including as early as 2013, with its publication "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value".¹⁵⁴ The OECD recognizes that data is a key competitive input not only in the digital economy but in all markets: "Big data now represents a core economic asset that can create significant competitive advantage for firms and drive innovation and growth."¹⁵⁵

344. As explained by Professors Acquisti, Taylor and Wagman in their 2016 article The Economics of Privacy:

Such vast amounts of collected data have obvious and substantial economic value. Individuals' traits and attributes (such as a person's age, address, gender, income, preferences, and reservation prices, but also her clickthroughs, comments posted online, photos uploaded to social media, and so forth) are increasingly regarded as business assets that can be used to target services or offers, provide relevant advertising, or be traded with other parties.¹⁵⁶

345. There is also a private market for users' personal information. One study by content marketing agency Fractl has found that an individual's online identity, including hacked financial

¹⁵³ *Id.*; see also Emily Steel et al., *How much is your personal data worth?*, FINANCIAL TIMES (June 12, 2013), <https://ig.ft.com/how-much-is-your-personal-data-worth/> (providing an estimate of values in 2013 of data regarding conditions such as ADHD, asthma, headaches and migraines, and others) (last visited Nov. 13, 2023).

¹⁵⁴ *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD DIGIT. ECON. PAPER No. 220 1, 7 (Apr. 2, 2013), <http://dx.doi.org/10.1787/5k486qtxldmq-en> (last visited Nov. 13, 2023).

¹⁵⁵ *Supporting Investment in Knowledge Capital*, Growth and Innovation, OECD PUBLISHING 1, 319 (Oct. 13, 2013), https://www.oecd-ilibrary.org/industry-and-services/supporting-investment-in-knowledge-capital-growth-and-innovation_9789264193307-en (last visited Nov. 13, 2023).

¹⁵⁶ Alessandro Acquisti, Curtis Taylor, and & Liad Wagman, *The Economics of Privacy*, 54 J. OF ECON. LITERATURE 442, 444 (June 2016), <https://www.heinz.cmu.edu/~acquisti/papers/AcquistiTaylorWagman-JEL-2016.pdf> (last visited Nov. 13, 2023).

accounts, can be sold for \$1,200 on the dark web.¹⁵⁷ These rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other users' content, surely users can sell their own. In short, there is economic value to users' data that is greater than zero. The exact number will be a matter for experts to determine.

1. License Value

346. Further, the ability to monetize personal information does not lie solely within "big data." Today, individuals can also monetize the value of their personal information. There are now market exchanges where individual users, like Plaintiffs and Class Members, can sell or monetize their own data.

347. For example, Nielsen Data, Killi, DataCoup, AppOptix and Mobile Computer will pay users for their data.¹⁵⁸

348. Similarly, Google itself has launched programs that pay users for their data. This includes a program called Screenwise -- an opt-in panel that can be installed on the Chrome Browser and permit Google to track and record individuals' browsing history in exchange for payment.¹⁵⁹ In a separate consumer data case against Google, the Court cited evidence that Google's Screenwise Panel collected the same types of information at issue in this case, i.e. content and identifiers that include cookies and device information, and that "participants are paid a baseline minimum of \$3 per month per device" that "does not decrease based on one's browsing activity[.]" *Brown v. Google*, 2022 WL 17961497, at *3-4 (N.D. Cal. Dec. 12, 2022).

¹⁵⁷ Maria LaMagna, *The Sad Truth About How Much Your Google Data is Worth on the Dark Web*, MARKETWATCH (June 6, 2018), <https://www.marketwatch.com/story/spooked-by-the-facebook-privacy-violations-this-is-how-much-your-personal-data-is-worth-on-the-dark-web-2018-03-20> (last visited Nov. 13, 2023).

¹⁵⁸ See e.g., Kevin Mercandante, *Ten Apps for Selling Your Data for Cash*, BEST WALLET HACKS (June 10, 2020), <https://wallethacks.com/apps-for-selling-your-data/> (last visited Nov. 13, 2023).

¹⁵⁹ Jack Marshall, *Google Pays Users for Browsing Data*, DIGIDAY (Feb. 10, 2012), <https://digiday.com/media/google-pays-users-for-browsing-data/> (last visited Nov. 13, 2023).

349. Likewise, apps such as Zynn, a TikTok competitor, pay users to sign up and interact with the app.¹⁶⁰

350. Google's services are not free. Rather than pay with cash, Google users pay for Google's services by agreeing to provide Google with the right to collect certain data, the "data license."

351. Google's "data license" right to collect data about its users is not unlimited.

352. The "data license" for Google's services is defined by law and Google's contract.

353. By law, Google may not collect Health Information about users without express informed consent on a form separate from the contract of adhesion that Google presents to users. Where Health Information is collected for marketing purposes, the legal requirements for its collection and use are even more stringent.¹⁶¹

354. Other limitations on the "data license" paid for Google's services are outlined by the Google contract.

355. The "data license" includes data that Google users provide when signing up for Google and when using Google platforms on Google's properties – subject to limitations in Google's contract.

¹⁶⁰ Jacob Kastrenakes, *A New TikTok Clone Hit the Top of the App Store by Paying Users to Watch Videos*, THE VERGE (May 29, 2020), <https://www.theverge.com/2020/5/29/21274994/zynn-tiktok-clone-pay-watch-videos-kuaishou-btyedance-rival> (last visited Nov. 13, 2023).

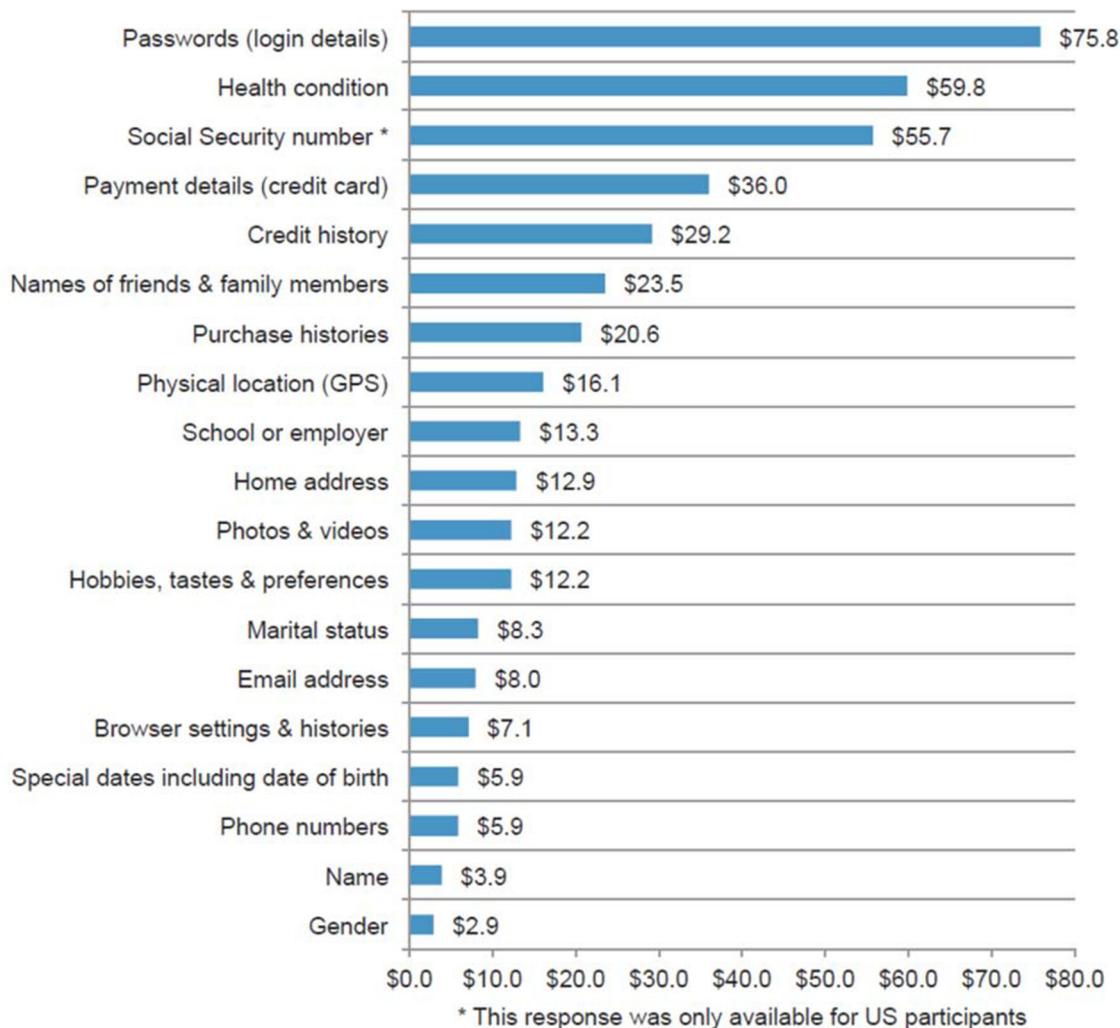
¹⁶¹ HIPAA prohibits covered entities from using or disclosing PHI for marketing purposes without "authorization," which must include, in "plain language," a description of the information to be used or disclosed, the name or other specific identification of the person authorized to make the requested use or disclosure, the name or other specific identification of the person to whom the covered entity may make the requested use or disclosure, a description of each purpose of the requested use or disclosure, an expiration date or event that relates to the individual or the purpose of the use or disclosure, the signature of the individual and the date, and statements that the individual has a right to revoke the authorization. 45 C.F.R. §164.508(a)(3). Further, Cal. Civ. Code § 1798.91 requires written consent from patients to use medical information for marketing purposes.

356. As described above, the “data license” does not include individual Health Information associated with a Google user and their Health Care Provider or other covered entities under federal and state health privacy laws.

357. Although not included in the contract, Google collects this additional data anyway, thereby overcharging Plaintiffs and Class Members for use of Google’s services.

358. The “data license” overcharge that Google collects without authorization, and the collected data, has monetary value.

359. For example, a 2015 study found respondents placed a value of \$59.80 on health information:¹⁶²



¹⁶² *Privacy and Security in a Connected Life: A Study of US, European and Japanese Consumers*,

360. In addition, some companies sell de-identified health information in the open market. For example, a company named Prognos Health provides a data platform where it purports to sell information from “more than 325 million de-identified patients.”¹⁶³

361. Google obtains substantial revenues from the collection and use of private health data for targeted ads.

362. In its Annual Form 10-K for the fiscal year ending December 31, 2022, filed with the Securities and Exchange Commission, Google reported total advertising revenue of \$224,473,000,000 for 2022, with 48% of this revenue attributable to United States users.¹⁶⁴

363. A 2019 study calculated the value of Americans’ personal information gathered and used by Google to be \$15.3 billion in 2016, \$18.1 billion in 2017, and \$21.5 billion in 2018.¹⁶⁵

364. Google and several other companies have products through which they pay consumers for a license to track certain information. Google, Nielsen, UpVoice, HoneyGain, and SavvyConnect are all companies that pay for browsing history information.

365. Ipsos, a global market research company, conducted a consumer research study called “Screenwise” on behalf of Google to learn “how people use the internet[.]”¹⁶⁶

PONEMON INSTITUTE, at 17 (March 2015), <https://perma.cc/V933-A6N3> (last visited Nov. 13, 2023).

¹⁶³ *Prognos Health Announces Patent-Pending Technology*, PROGNOS HEALTH (Apr. 6, 2021 1:36 PM EST), <https://www.prnewswire.com/news-releases/prognos-health-announces-patent-pending-technology-301263364.html> (last visited Nov. 13, 2023).

¹⁶⁴ *Annual Report (Form 10-K)*, ALPHABET, INC., at 59 (Dec. 31, 2022), https://abc.xyz/investor/static/pdf/20230203_alphabet_10K.pdf?cache=5ae4398 (last visited Nov. 13, 2023).

¹⁶⁵ Robert Shapiro & Siddhartha Aneja, *Who Owns Americans’ Personal Information and What Is It Worth?*, FUTURE MAJORITY, at 3 (March 2019), <https://assets.futuremajority.org/uploads/report-for-future-majority-on-the-value-of-people-s-personal-data-shapiro-aneja-march-8-2019.pdf> (last visited Nov. 13, 2023).

¹⁶⁶ *Ipsos Screenwise Panel*, IPSOS, <https://screenwisepanel.com> (last visited Nov. 13, 2023).

366. The Screenwise study paid participants \$20 for qualifying for the study, an additional \$100 if the participant joined and installed a special WiFi router, and an additional \$16 per month for each household member who joined with their device.¹⁶⁷

367. Because Americans typically do not want to sell their individually identifiable health information for any purpose and it is illegal to even share it without express, written authorization, there are fewer open markets for a license to collect or sell individually identifiable health information for non-health purposes than other types of data. However, black markets do exist for such data. It has been reported that health data can be “more expensive than stolen credit card numbers” on black markets.¹⁶⁸

368. While the exact value of Plaintiffs’ and Class Members’ Health Information in this action will be a matter for expert determination, it is clear that its value is substantial.

2. Individuals Have a Protectable Property Interest in Their Health Information.

369. Property is the right of any person to possess, use, enjoy, or dispose of a thing, including intangible things like data and communications.

370. The Health Information at issue here is property under California law. *See, e.g. Calhoun, et al. v. Google, LLC*, 526 F. Supp. 3d. 605, 635 (N.D. Cal. 2021) (“users have a property interest in their personal information”); *People v. Kwok*, 75 Cal. App. 4th 1236, 1251 (1998) (property includes a copy of a key that is made without the key owner’s knowledge when the original is returned to the owner, “which is analogous to making … an unauthorized copy of computer data”).¹⁶⁹

¹⁶⁷ *Id.*

¹⁶⁸ Aarti Shahani, *The Black Market for Stolen Health Care Data*, NPR: ALL TECH CONSIDERED, at 3 (Feb. 13, 2015 4:55 AM ET), <https://www.npr.org/sections/alltechconsidered/2015/02/13/385901377/the-black-market-for-stolen-health-care-data> (last visited Nov. 13, 2023).

¹⁶⁹ *See also Fields v. Michael*, 91 Cal. App. 2d 443, 449 (1949) (“[t]he word property may be properly used to signify any valuable right or interest protected by law”); *Downing v. Municipal Court*, 88 Cal. App. 2d 345, 359 (1948) (same); *Yuba River Power Co. v. Nevada Irr. Dist.*, 207 Cal. 521, 523 (1920) (“[t]he term property is sufficiently comprehensive to include every species of estate, real and personal, and everything which one person can own and transfer to another. It

371. Indeed, federal and state law grant patients the right to protect the confidentiality of data that identifies them as patients of a particular health care provider and restrict the use of their health data, including their status as a patient, to only uses related to their care or otherwise authorized by federal or state law in the absence of patient authorization. *See, e.g.*, HIPAA, CMIA, CCPA.

372. Likewise, American courts have long recognized common law property rights in the content of a person's communications that are not to be used or disclosed to others without authorization. *See, e.g.*, ECPA; Title III (the Pen Register Act); *Folsom v. Marsh*, 9 F.Cas. 342, 346 (C.C.D. Mass. 1841) (recognizing common law information property rights) (Story, J); *Baker v. Libbie*, 210 Mass. 599, 602 (1912) (same); *Denis v. LeClerc*, 1 Mart. (La.) 297 (1811) (same).

373. Google's taking of individuals' Health Information without authorization is done in violation of individuals' protected property interest in this information. It is an unlawful taking – larceny – under California law regardless of whether and to what extent Google monetized the data, and individuals have a right to disgorgement and/or restitution damages for the value of the stolen data.

374. In addition, with respect to Google Account Holders, who entered into contractual agreements with Google, they have suffered benefit of the bargain damages in that Google took more data than the parties agreed would be exchanged. Those benefit of the bargain damages also include, but are not limited to: (i) loss of the promised benefits of their Google Account Holder experience; (ii) out-of-pocket costs; and (iii) loss of control over property which has marketable value.

375. Plaintiffs seek restitution for the unjust enrichment obtained by Google as a result of unlawfully collecting Plaintiffs' personal Health Information. These intrusions are highly offensive to a reasonable person. Further, the extent of the intrusion cannot be fully known, as the

extends to every species of right and interest capable of being enjoyed as such upon which it is practicable to place a money value"); *People v. Kozlowski*, 96 Cal. App. 4th 853, 866 (2002) ("[t]he term [property] is all-embracing, including every intangible benefit and prerogative susceptible of possession or disposition").

nature of privacy invasion involves sharing Plaintiffs' and Class Members' Health Information with potentially countless third parties, known and unknown, for undisclosed and potentially unknowable purposes, in perpetuity. Also supporting the highly offensive nature of Google's conduct is the fact that Google's principal goal is and was to surreptitiously monitor Plaintiffs and Class Members and to allow third parties to do the same.

V. CLASS ACTION ALLEGATIONS

376. Plaintiffs file this as a class action on behalf of themselves and the following class and subclass:¹⁷⁰

ALL U.S. HEALTH USER CLASS – All persons in the United States and its territories whose Health Information was obtained by Google from their Health Care Provider.

GOOGLE ACCOUNT HOLDER SUBCLASS – All Google Account Holders in the United States and its territories whose Health Information was obtained by Google from their Health Care Provider.

377. As used in this Complaint, the phrase "Health Care Provider" includes all health care providers, covered entities, and business associates whose information is protected by HIPAA or the CMIA. *See* 45 C.F.R. § 160.103; Cal. Civ. Code § 56. This includes doctors, clinics, psychologists, dentists, chiropractors, nursing homes, pharmacies, health insurance companies, pharmaceutical companies, and business associates such as vendors Cerner and Epic that operate online patient portals. *See id.*

378. As used in this Complaint, the phrase "Health Information" includes an individual's status as a patient of a Health Care Provider, unique patient identifiers, the specific actions taken by patients on their Health Care Provider web properties (e.g. specific time and frequency of each patient interaction, such as when a patient logs in to and logs out of an online patient portal, requests an appointment, or seeks information about a specific doctor, condition, treatment, or prescription drug), and content of communications that patients exchange with their Health Care Providers. Content information, in turn, includes information pertaining to patient registrations,

¹⁷⁰ Plaintiffs reserve the right to modify the Class and Subclass Definition at the class certification stage or as otherwise instructed by the Court.

access to, and communications with their Health Care Provider within authenticated webpages (i.e., webpages that require log-in or other authentication, such as a patient portal), as well as content information pertaining to patient access to and communications with their Health Care Provider on unauthenticated web pages (e.g., communications relating to specific doctors, appointment requests, symptoms, conditions, treatments, insurance, and prescription drugs).

379. Excluded from the Class are the Court and its personnel and the Defendant and its officers, directors, employees, affiliates, legal representatives, predecessors, successors and assigns, and any entity in which any of them has a controlling interest.

380. The members of the Class are so numerous that joinder is impracticable.

381. Common questions of law and fact are apt to drive resolution of the case, exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class including, but not limited to, the following:

- a. Whether Google unlawfully collects Health Information;
- b. Whether Google uses Health Information for advertising purposes;
- c. Whether the Google Terms of Service includes binding contractual promises;
- d. Whether the Google Privacy Policy includes binding contractual promises;
- e. Whether Google's tracking, collection and/or monetization of Health Information constitutes a breach of contract with Google Account Holders;
- f. Whether Google had legal authorization to acquire Class Members Health Information;
- g. Whether Class Members have a reasonable expectation of privacy over their Health Information;
- h. Whether Google's tracking, collection, and/or monetization of Health Information constitutes highly offensive conduct;
- i. Whether Google was unjustly enriched as a result of its violations of Plaintiffs' and Class Members' privacy rights;

- j. Whether the Health Information at issue is “content” under the ECPA;
- k. Whether the Health Information at issue has economic value; and
- l. Whether Google unjustly profited from the conduct alleged herein.

382. Plaintiffs’ claims are typical of the claims of other Class Members, as all members of the Classes were similarly affected by Google’s wrongful conduct in violation of federal and California law, as complained of herein.

383. Plaintiffs will fairly and adequately protect the interests of the members of the Classes and have retained counsel that is competent and experienced in class action litigation. Plaintiffs have no interests that conflict with, or are otherwise antagonistic to, the interests of other Class Members.

384. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. Further, as the damages that individual Class Members have suffered may be relatively small, the expense and burden of individual litigation make it impossible for members of the Class to individually redress the wrongs done to them. There will be no difficulty in management of this action as a class action.

VI. TOLLING

385. Any applicable statute of limitations has been tolled by Defendant’s knowing and active concealment of the conduct and misrepresentations and omissions alleged herein. Through no fault or lack of diligence, Plaintiffs and members of the Classes were deceived and could not reasonably discover Defendant’s deception and unlawful conduct.

386. Plaintiffs and members of the Classes did not discover and did not know of any facts that would have caused a reasonable person to suspect that Defendant was acting unlawfully and in the manner alleged herein. As alleged herein, the representations made by Google were material to Plaintiffs and members of the Classes at all relevant times. Within the time period of any applicable statutes of limitations, Plaintiffs and members of the Classes could not have discovered through the exercise of reasonable diligence the alleged wrongful conduct.

387. Particularly in light of the sensitivity of Health Information as a category, privacy expectations rooted in federal and state law regarding such information, and the invisibility of Google Source Code on affected web properties, at all times, Defendant is and was under a continuous duty to disclose to Plaintiffs and members of the Classes the true nature of the disclosures being made and the lack of an actual “requirement” before the data was shared with it.

388. Defendant knowingly, actively, affirmatively and/or negligently concealed the facts alleged herein. Plaintiffs and members of the Classes reasonably relied on Defendant’s concealment.

389. Further, Defendant’s unlawful tracking, collection, and monetization of Plaintiffs and Class Members’ Health Information was done surreptitiously in a manner undetectable by patients. As a result, despite Plaintiffs and Class Members exercise of due diligence, they could not, and did not, discover the unlawful conduct described herein.

390. Plaintiffs only became aware of Google’s wrongdoing alleged herein shortly before the filing of this complaint as a result of counsel’s investigation.

391. For these reasons, all applicable statutes of limitation have been tolled based on the discovery rule and Defendant’s concealment, and Defendant is estopped from relying on any statutes of limitations in defense of this action.

VII. CAUSES OF ACTION

COUNT ONE **VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT** **(On Behalf of All Classes)**

392. Plaintiffs hereby incorporate the factual allegations set forth above by reference.

393. The ECPA prohibits the intentional interception of the contents of any electronic communication. 18 U.S.C. § 2511.

394. Under the Act, an “electronic communication” is defined as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.”

395. The Plaintiffs communications with Health Care Provider web-properties described herein are “electronic communications” under the Act.

396. Under the Act, “interception” is defined as the “acquisition of the contents of any ... electronic communication ... through the use of any ... device.”

397. The ECPA protects both the sending and receiving of communications and provides a private right of action to any person whose electronic communications are intercepted. *See* 18 U.S.C. § 2520(a).

398. Google intentionally intercepted, i.e. acquired, Plaintiffs’ and Class Members’ Health Information on their Health Care Providers’ web properties where the Google Source Code was present.

399. Google’s acquisition of Health Information was contemporaneous with their making.

400. The Act expressly states that communications “contents ... includes any information concerning the substance, purport, or meaning of that communication.”

401. As alleged herein, the transmissions of Health Information between Plaintiffs and Class Members and their Health Care Providers qualify as “contents” of communications under the ECPA’s definition. The intercepted communications contents includes, but is not limited to:

- a. the precise content of patient registrations, including information that Plaintiffs and patient input into online forms in the process of patient registration and communications exchanged during the registration to indicate patient status and sign-ups;
- b. the precise content of patients’ access to and communications with their Health Care Provider within authenticated patient portals, such as logging-in or logging out of a patient portal and exchanging communications about appointments, treatments, conditions, allergies, medical records, payments, or providers inside the portals;

- c. the precise content of searches that patients conduct on Health Care Provider web properties for providers, treatments, conditions, payment information, insurance, and more; and
- d. the precise content of patients' access to and communications with their Health Care Provider on pages directed towards patients outside of the patient portal, which include communications relating to specific doctors, symptoms, conditions, treatments, prescription drugs, and requests for appointments.

402. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

- a. The Google Cookies used to track patients' communications;
- b. Patients' browsers;
- c. Patients' computing devices;
- d. Google's web-servers;
- e. The web-servers of Health Care Providers' web properties where the Google Source Code was present; and
- f. The Google Source Code deployed by Google to effectuate its acquisition of patient communications.

403. Google is not a party to Plaintiffs' and Class Members' communications with their Health Care Providers.

404. Google intercepted and received Plaintiffs' and Class Members' Health Information through the surreptitious redirection from Plaintiffs' and Class Members' computing devices to Google via the Google Source Code.

405. Neither Google nor the Health Care Providers obtained Plaintiffs' and Class Members' lawful consent or authorization for Google's acquisition of Health Information.

406. Google did not require any Health Care Provider to obtain lawful rights to share Plaintiffs' and Class Members' Health Information with Google.

407. Any purported consent that Google received from Health Care Providers to obtain Plaintiffs' and Class Members' Health Information was not valid.

408. In acquiring Plaintiffs' and Class Members' Health Information, Google had a purpose that was tortious, criminal, and designed to violate constitutional and statutory provisions including, but not limited to:

- a. The unauthorized acquisition of individually identifiable health information is tortious in and of itself regardless of whether the means deployed to acquire the information violates the Wiretap act or any subsequent purpose or use for the acquisition. Google intentionally committed a tortious act by acquiring individually identifiable health information without authorization to do so;
- b. The unauthorized acquisition of individually identifiable health information is a criminal violation of 42 U.S.C. § 1320d-6 regardless of any subsequent purpose or use of the individually identifiable health information. Google intentionally violated 42 U.S.C. § 1320d-6 by intentionally acquiring individually identifiable health information without authorization;
- c. A violation of HIPAA, particularly 42 U.S.C. § 1320d-6, which is a criminal offense punishable by fine or imprisonment with increased penalties where “the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage [or] personal gain.” Google intentionally violated the enhanced penalty provision of 42 U.S.C. § 1320d-6 by acquiring the individually identifiable health information “with intent to sell transfer or use” it for “commercial advantage [or] personal gain”;
- d. To the extent that any particular at-issue communication or web-property may be found to not be protected by HIPAA, Google’s conduct is also prohibited by the FTC Act, as codified at 15 U.S.C. § 45, which provides that “unfair or deceptive acts or practices in or affecting commerce, are hereby declared illegal”;
- e. A knowing intrusion upon Plaintiffs' and Class Members' seclusion;
- f. Trespass upon Plaintiffs' and Class Members' personal and private property via the placement of Google Cookies associated with the domains and patient

portals for their Health Care Providers and covered entities on Plaintiffs' and Class Members' personal computing devices;

- g. Violation of the California Unfair Competition Law;
- h. Violation of the California Constitution's right to privacy, Section 1 of Article I of the California Constitution;
- i. Violation of various state privacy statutes including, but not limited to, the CMIA; CCPA; CIPA, and Cal. Civ. Code § 1798.91;
- j. Violation of various state computer privacy and property statutes, including but not limited to the California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502; and,
- k. Violation of Cal. Penal Code § 484 for statutory larceny.

409. Any purported consent provided by Health Care Providers had a purpose that was tortious, criminal, and in violation of state constitutional provisions, in that such conduct by the Health Care Provider constitutes:

- a. A knowing intrusion into a private place, conversation, or matter that would be highly offensive to a reasonable person;
- b. A violation of HIPAA, 42 U.S.C. § 1320d-6, which is a criminal offense punishable by fine or imprisonment and that includes increased penalties where “the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage [or] personal gain”;
- c. Trespass;
- d. Breach of fiduciary duty; and
- e. Violation of various state privacy statutes including, but not limited to, the CMIA; CCPA; CIPA; and Cal. Civ. Code § 1798.91.

410. Google knows that its collection of Health Information from Health Care Providers is unlawful and tortious and provides public proof of such knowledge with its webpage titled “HIPAA and Google Analytics,” which expressly states: “[c]ustomer[s] must refrain from using

Google Analytics in any way that may create obligations under HIPAA for Google” and that “Google makes no representations that Google Analytics satisfies HIPAA requirements and does not offer Business Associate Agreements in connection with this service.” Google further states that:

- a. “Customers who are subject to HIPAA must not use Google Analytics in any way that implicates Google’s access to, or collection of [protected health information], and may only use Google Analytics on pages that are not HIPAA-covered.”;
- b. “Authenticated pages are likely to be HIPAA-covered and customers should not set Google Analytics tags on those pages.”; and
- c. “Unauthenticated pages that are related to the provision of health care services, including as described in the HHS bulletin, are more likely to be HIPAA-covered, and customers should not set Google Analytics tags on HIPAA-covered pages.”

411. Despite these statements, Google takes no further actions to identify and prevent the collection of Health Information from Health Care Providers. Instead, Google tracks, collects, and monetizes Health Information with full knowledge that it was collected in violation of HIPAA, which gives rise to criminal liability under 42 U.S.C. § 1320d-6, and various other state and common law torts and statutory causes of action listed herein.

412. Google’s violations of the ECPA were willful and intentional and caused Plaintiffs and Class Members the following damages:

- a. The interruption or preclusion of Plaintiffs’ and Class Members’ ability to communicate with their Health Care Providers;
- b. The diminution in value of Plaintiffs’ and Class Members’ Health Information;
- c. The inability to use their computing devices for the purpose of communicating with their Health Care Providers;

- d. The loss of privacy due to Google making sensitive and confidential information, such as patient status, medical issues, and appointments, that Plaintiffs and Class Members intended to remain private no longer private; and
- e. Google took something of value from Plaintiffs and Class Members and derived benefits therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without Google sharing the benefit of such value.

413. For Google's violations set forth above, Plaintiffs and Class Members seek appropriate equitable and declaratory relief, including injunctive relief; actual damages and any profits made by Google as a result of its violations or the appropriate statutory measure of damages; punitive damages in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred pursuant to 18 U.S.C. § 2520.

414. Unless enjoined, Google will continue to commit the violations of law alleged here. Plaintiffs and Class Members want to continue to communicate with their Health Care Providers through online platforms but have no practical way of knowing if their communications are being intercepted by Google, and thus continue to be at risk of harm from Google's conduct.

415. Pursuant to 18 U.S.C. § 2520, Plaintiffs and Class Members seek monetary damages for the greater of (i) the sum of the actual damages suffered by the Plaintiffs and any profits made by Google as a result of the violation or (ii) statutory damages of whichever is greater of \$100 a day for each violation or \$10,000.

COUNT TWO
VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT
(On Behalf of All Classes)

416. Plaintiffs hereby incorporate the factual allegations set forth above by reference.

417. CIPA is codified at Cal. Penal Code §§ 630-638. The Act begins with the following statement of purpose:

The legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and

civilized society.

Cal. Penal Code § 630.

418. Cal. Penal Code § 631(a) provides, in pertinent part:

Any person who, by means of any machine, instrument, or contrivance, or in any other manner willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to lawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars.

419. There are no “vendor” or “agent” exceptions under Cal. Pen. Code § 631.

420. Cal. Penal Code § 632 provides, in pertinent part, that it is unlawful for any person “intentionally and without the consent of all parties to a confidential communication,” to “use[] [a] recording device to ... record the confidential communication.”

421. As used in the statute, a “confidential communication” is:

any communication carried on in circumstances as may reasonably indicate that any party to the communication desired it to be confined to the parties thereto[.]

422. Plaintiffs’ and Class Members’ Health Information, which was communicated with their Health Care Providers, constitutes confidential communications within the meaning of CIPA.

423. The Google Source Code constitutes a “device” within the meaning of CIPA § 632.

424. There are no “vendor” or “agent” exceptions under Cal. Pen. Code § 632.

425. Google is a “person” within the meaning of CIPA §§ 631 and 632.

426. Google is headquartered in California, designed, contrived, and effectuated its scheme to track, intercept, store, share and sell Plaintiffs’ and Class Members’ Health Information from California, and has adopted California substantive law to govern its relationship with users.

427. Google did not have the prior consent or authorization of all parties to obtain Plaintiffs’ and Class Members’ Health Information exchanged with their Health Care Providers, which includes the contents or record of their confidential communications.

428. Google's actions were designed to learn or attempt to learn the contents of Plaintiffs' and Class Members' electronic communications with their Health Care Providers.

429. Google's learning of or attempt to learn of the contents of Plaintiffs' and Class Members' electronic communications with Health Care Providers occurred while the communications were in transit or in the process of being sent or received.

430. Unless enjoined, Google will continue to commit the violations of law alleged here. Plaintiffs want to continue to communicate with their Health Care Providers and covered entities through online platforms but have no practical way of knowing if their communications are being intercepted by Google, and thus continue to be at risk of harm from Google's conduct.

431. Plaintiffs and Class Members seek all relief available under Cal. Penal Code § 637.2, including injunctive relief and statutory damages of \$5,000 per violation or three times the actual amount of damages.

COUNT THREE
CALIFORNIA CONSTITUTIONAL INVASION OF PRIVACY
(On Behalf of All Classes)

432. Plaintiffs hereby incorporate the factual allegations set forth above by reference.

433. The California Constitution provides:

All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.

Cal. Const. art. I, § 1 (emphasis added).

434. Plaintiffs and Class Members have both an interest in precluding the dissemination and misuse of their Health Information by Google, and in making intimate personal decisions and communicating with Health Care Providers without observation, intrusion or interference by Google.

435. Plaintiffs and Class Members had no knowledge of and did not consent or authorize Google to obtain their Health Information as described herein.

436. Plaintiffs and Class Members enjoyed objectively reasonable expectations of privacy surrounding their Health Information and communications devices used to exchange communications with their Health Care Providers, as evidenced by, among other things, federal, state and common laws that uphold the confidentiality of such information and that require lawful consent prior to disclosure.

437. Plaintiffs' and Class Members' claims are based on Google's unauthorized access to their Health Information as alleged herein, which includes, but is not limited to:

- a. Plaintiffs' and Class Members' status as patients of a particular Health Care Provider;
- b. Plaintiffs' and Class Members' communications while logged-in to "authenticated" pages on the Health Care Provider web properties, including the specific and detailed content of such communications, such as search terms, requests and responses for communications about appointments, doctors, treatments, conditions, health insurance, prescription drugs, and other Health Information;
- c. Plaintiffs' and Class Members' communications with their Health Care Providers on "unauthenticated" portions of those properties, including the specific and detailed content of such communications, such as search terms and requests and responses for communications requesting information about appointments, doctors, treatments, conditions, health insurance, prescription drugs, and other Health Information; and
- d. The ability to control and deny access to their communications devices while exchanging communications with their Health Care Providers on authenticated or unauthenticated pages.

438. In addition to acquiring Health Information without authorization, Google violated Plaintiffs' and Class Members' right to privacy in their communications devices by configuring

Google Source Code to deposit and disguise Google Cookies as “first-party” cookies belonging to Health Care Providers, when, in fact, they are third-party cookies belonging to Google.

439. Google’s conduct was intentional and intruded on Plaintiffs’ and Class Members’ communications with their Health Care Providers, which constitute private conversations, matters, and data.

440. Google’s conduct was highly offensive because, among other things:

- a. Google conspired with Health Care Providers to violate a cardinal rule of the provider-patient relationship;
- b. Google’s conduct violated federal and state law designed to protect patient privacy, including but not limited to HIPAA and the CMIA;
- c. Google’s conduct violated the express promises it made to Google Account Holders; and
- d. Google’s conduct violated implied promises made to all users that it would not participate, enable, encourage, or profit from unlawful activity against Plaintiffs and Class Members.

441. Google’s invasion of Plaintiffs’ and Class Members’ privacy resulted in the following damages:

- a. Nominal damages for invasion of privacy;
- b. General damages for invasion of their privacy rights in an amount to be determined by a jury without reference to specific pecuniary harm;
- c. The interruption or preclusion of Plaintiffs’ and Class Members’ ability to communicate with their Health Care Providers on their Health Care Providers’ web properties;
- d. The diminution in value of Plaintiffs’ and Class Members’ Health Information;
- e. Plaintiffs’ and Class Members’ inability to use their computing devices for the purpose of communicating with their Health Care Providers;

- f. Sensitive and confidential information including patient status and appointments that Plaintiffs and Class Members intended to remain private are no longer private;
- g. Google eroded the essential confidential nature of the patient-provider relationship; and
- h. Google took something of value from Plaintiffs and Class Members and derived benefits therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without sharing the benefit of such value.

COUNT FOUR
INTRUSION UPON SECLUSION
(On Behalf of All Classes)

- 442. Plaintiffs hereby incorporate the factual allegations set forth above by reference.
- 443. By collecting and using the contents of Plaintiffs' and Class Members' communications with their Health Care Providers and covered entities without their knowledge, Google intentionally intruded into a realm in which Plaintiffs and Class Members have a reasonable expectation of privacy.
- 444. Plaintiffs and Class Members enjoyed objectively reasonable expectations of privacy in their communications with their Health Care Providers and covered entities relating to the respective patient portals, appointments, and Health Information and communications based on:
 - a. The Health Care Providers' or covered entities' status as their Health Care Providers or a covered entity and the reasonable expectations of privacy that attach to patient-provider relationships;
 - b. HIPAA;
 - c. The ECPA;
 - d. Google's promises that it will not use, or allow advertisers to use, Plaintiffs' and Class Members' Health Information for personalized advertising; and
 - e. California medical and computer privacy laws.

445. Furthermore, Plaintiffs and Class Members maintained a reasonable expectation of privacy when providing their Health Information to their Health Care Providers and covered entities and when communicating with their Health Care Providers and covered entities online.

446. Health Information is widely recognized by society as sensitive information that cannot be shared with third parties without the patients' consent.

447. For example, polling shows that “[n]inety-seven percent of Americans believe that doctors, hospitals, labs and health technology systems should not be allowed to share or sell their sensitive health information without consent.”¹⁷¹

448. Google obtained unwanted access to Plaintiffs' and Class Members' Health Information, including, but not limited, to their patient status, the dates and times Plaintiffs and Class Members logged in to or out of patient portals, and the communications Plaintiffs and Class Members exchanged while logged in to patient portals.

449. In addition, Google intruded upon Plaintiffs' and Class Members' computing devices by gaining unauthorized access to those devices via web-bugs and “ghost cookies,” i.e. cookies that are nominally set by the Health Care Provider web-property to get around any efforts to prevent companies like Google from tracking consumers but that, in reality, belong to and are used by Google to surveil the Plaintiffs and Class Members.

450. Google's intrusion was accomplished by placing the _ga, _gid, __gcl_au, NID, IDE, DSID, and direct Google Account cookies on Plaintiffs' and Class Members' computing devices through the web-servers of Plaintiffs' and Class Members' Health Care Providers.

451. By disguising the _ga, _gid, and __gcl_au cookies as first-party cookies from Plaintiffs' Health Care Providers or covered entities, Google ensures that it can hack its way around attempts that Plaintiffs and Class Members might make to prevent Google's tracking through the use of cookie blockers.

¹⁷¹ *Poll: Huge majorities want control over health info*, HEALTHCARE FINANCE, at 1 (Nov. 10, 2010), <https://www.healthcarefinancenews.com/news/poll-huge-majorities-want-control-over-health-info> (last visited Nov. 13, 2023).

452. In designing cookies as disguised first-party cookies, Google was aware that, like other websites that include sections where users sign in to an account, any Health Care Provider or covered entity website with a patient portal would require first-party cookies to be enabled for a patient to access the patient portal or other username / password protected ‘secure’ part of the Health Care Provider’s website.

453. With first-party cookies being required for use of a patient portal and the Google cookies disguised as first-party cookies, Google was able to implant its tracking device on the computing devices of Plaintiffs and Class Members even where Plaintiffs or Class Members made attempts to stop third-party tracking through the use of cookie blockers.

454. Google’s deployment of third-party cookies disguised as first-party cookies that are placed on Plaintiffs’ and Class Members’ computing devices is a highly offensive intrusion upon seclusion regardless of whether any information was further redirected from Plaintiffs’ or Class Members’ computing devices to Google.

455. Google’s intrusion into Plaintiffs’ and Class Members’ privacy would be highly offensive to a reasonable person, namely because it occurred without Plaintiffs’ and Class Members’ consent or knowledge.

456. Google’s intrusion caused Plaintiffs and Class Members the following damages:

- a. Nominal damages;
- b. The interruption or preclusion of Plaintiffs’ and Class Members’ ability to communicate with their Health Care Providers on their Health Care Providers’ web properties;
- c. The diminution in value of Plaintiffs’ and Class Members’ protected health information;
- d. The inability to use their computing devices for the purpose of communicating with their Health Care Providers;

- e. The loss of privacy due to Google making sensitive and confidential information such as patient status and appointments that Plaintiffs and Class Members intended to remain private no longer private; and
- f. Google took something of value from Plaintiffs and Class Members and derived benefits therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without Google sharing the benefit of such value.

457. Google's intrusion into Plaintiffs' and Class Members' seclusion was with oppression, fraud, or malice.

458. For Google's intrusion into their seclusion, Plaintiffs and Class Members seek actual damages, compensatory damages, restitution, disgorgement, general damages, nominal damages, unjust enrichment, punitive damages, and any other relief the Court deems just.

COUNT FIVE
VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW
(On Behalf of All Classes)

459. Plaintiffs hereby incorporate the factual allegations set forth above by reference.

460. California Business and Professions Code, Section 17200, ("UCL") prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising . . .".

461. Google engaged in unlawful and unfair business acts and practices in violation of the UCL.

462. Unlawful: Google has engaged in unlawful acts or practices in that the conduct alleged herein constitutes violations of, among other things:

- a. the California Constitution's right to privacy;
- b. the ECPA;
- c. HIPAA, including specifically 42 U.S.C. § 1320d-6; and
- d. California health and computer privacy statutes, including but not limited to CMIA; CCPA; CIPA; and Cal. Civ. Code § 1798.91.

463. Unfair: Google engaged in unfair acts and practices in that Google assures users of all Google products that it will not collect Health Information without users' consent but in reality knows (or should have known) that the Google Source Code and advertising products are being improperly used on Health Care Provider web properties resulting in the wrongful, contemporaneous, redirection to Google of Plaintiffs' and Class Members' Health Information without their knowledge or consent.

464. Google's conduct as alleged herein offends public policy, including California's public policy of protecting consumer data.

465. Google's conduct, misrepresentations and omissions have also impaired competition within the health care market in that Google's conduct prevented Plaintiffs and Class Members from making fully informed decisions about whether to communicate online with their Health Care Providers and to use their Health Care Providers' websites in the first instance.

466. Plaintiffs and Class Members suffered an injury in fact, including the loss of money and/or property, as a result of Google's unfair, unlawful and deceptive practices. Plaintiffs' and Class Members' Health Information has undeniable value as demonstrated by the fact that Google is able to use and sell this information within its various advertising systems. While only an identifiable "trifle" of injury is needed to be shown, as set forth herein Plaintiffs, Class Members, and the public at large value their Health Information at more than a "trifle" amount. And Google's disclosure of this confidential and valuable information has now diminished the value of such information to Plaintiffs and Class Members.

467. Google's actions caused damage to and loss of Plaintiffs' and Class Members' property right to control the dissemination and use of their Health Information.

468. Plaintiffs and Class Members relied on Google's representation that it will not collect Health Information without users' consent.

469. Google's representation that it will not collect Health Information without users' consent was untrue.

470. Had Plaintiffs and Class Members known the truth of Google's conduct, they would not have used the Health Care Provider web properties in the way that they did or not used them at all, if possible.

471. The wrongful acts alleged herein occurred, and continues to occur, in the conduct of Google's business. Google's misconduct is part of a pattern or generalized course of conduct that is still perpetuated and repeated in the State of California.

472. Plaintiffs and Class Members want to continue using their Health Care Providers' web properties to communicate with their Health Care Providers, request and set appointments, and complete other tasks that necessary to access health care services and maintain their health.

473. If it does not change its practices, Google will continue to contemporaneously obtain Plaintiffs' and Class Members' Health Information.

474. Plaintiffs and Class Members will have no way to discern, while using their current or future Health Care Providers' web properties, whether Google is contemporaneously obtaining their individually identifiable health information and communications.

475. In addition, because the Google Cookies masquerade as first-party cookies to evade third-party cookie blockers, Plaintiffs and Class Members cannot manually block Google Cookies so as to protect the confidentiality of their data and communications.

476. As a result, the threat of future injuries identical to those that Google has already inflicted on Plaintiffs and Class Members is actual and imminent for Plaintiffs and Class Members.

477. Plaintiffs and Class Members request that this Court enjoin Google from continuing its unfair, unlawful, and deceptive practices and to restore to Plaintiffs and Class Members, in the form of restitution, any money Google acquired through its unfair, unlawful, and deceptive practices.

478. The injuries of Plaintiffs and Class Members cannot be wholly remedied by monetary relief and such remedies at law are inadequate.

COUNT SIX
TRESPASS TO CHATTELS
(On Behalf of All Classes)

479. Plaintiffs hereby incorporate the factual allegations set forth above by reference.

480. At all times relevant, Plaintiffs owned, leased, occupied, and/or controlled their computing devices. The chattels at issue in this claim are Plaintiffs' computing devices.

481. Plaintiffs purchased and/or leased their computing devices with the expectation that only Plaintiffs or those authorized by Plaintiffs would use the devices, gain access to, or deposit items on the device for any purpose; that only Plaintiffs or those authorized by Plaintiffs would gain access to Health Care information pertaining to Plaintiffs through use of Plaintiffs' devices; and that the devices could be used as a means of online communication with other individuals and entities at Plaintiffs' discretion, including Health Care Providers, without divulging information about those communications to third parties.

482. The Google Source Code is designed such that when Plaintiffs and Class Members visit their Health Care Providers' web properties Google Cookies are automatically set upon, thereby trespassing into, Plaintiffs' and Class Members' computing devices.

483. Google designed its source code for the purpose of lodging Google Cookies on computing devices such as Plaintiffs' and Class Members' and with knowledge that such lodging would, with substantial certainty, result from Google's actions in designing Google Source Code as it did and making the Source Code available to Health Care Provider websites as designed.

484. The Google Cookies are designed to avoid any attempts by Plaintiffs and Class Members to block transmissions to Google. To accomplish this task, the Google Source Code transmits and commands Google Cookies to be lodged in Plaintiffs' and Class members' computing devices by disguising the Google Cookies to be from their Health Care Providers. Thus, the Google Source Code is able to place the Google Cookies on Plaintiffs' and Class Members' computing devices regardless of whether Plaintiffs or Class Members have attempted to block third-party cookies.

485. The consequence of this false “first party” cookie designation to Plaintiffs and Class Members is that, for security purposes, Plaintiffs and Class Members must enable first-party cookies to communicate with their Health Care Providers’ web properties. As a result of this, every patient who accessed a patient portal for a Health Care Provider that deployed the Google Source Code had Google Cookies lodged on their computing device.

486. Google’s placement of Google Cookies associated with Plaintiffs’ and Class Members’ communications on Health Care Providers’ web properties was done intentionally and without Plaintiffs’ and Class Members’ knowledge or authorization.

487. The consequences of Google Cookies’ trespass into Plaintiffs’ computing devices include that Google uses the devices to gain access to Health Care information pertaining to Plaintiffs, and the devices cannot be used as a means of online communication with Health Care Providers without divulging information about those communications to Google.

488. In addition, the Google Cookies and the methods through which Google commands patient devices to re-direct patient identifiers and communications content in the middle of a patient’s communication with their Health Care Provider reduces storage, disk space, and performance of Plaintiffs’ and Class Members’ computing devices in a measurable way.

489. In the absence of the Google Source Code and Google Cookies, the Named Plaintiffs’ and Class members’ computing devices would have more storage available.

490. The Google Source Code and Google Cookies diverted a measurable amount of the resources available for the exchange of communications between patients and their Health Care Providers, slowing the speed of those communications and efficiency of the Plaintiffs’ and Class members’ computing devices in a measurable amount.

491. Had they known of Google’s trespass in the first instance, persons of ordinary sensibilities, including Plaintiffs and Class Members, would have regarded their devices as utterly incapable of their expected uses. Plaintiffs and Class Members now do regard their devices as utterly incapable of their expected uses because they have been compromised without Plaintiffs’ and Class Members’ knowledge in the past and because Google’s placement of Google Cookies

results in the persistent and unavoidable interception of Plaintiffs' and Class Members' communications with Health Care Providers.

492. Plaintiffs' and Class Members' devices are useless to persons of ordinary sensibilities for exchanging private communications with Health Care Providers where Google Source Code is deployed on the Health Care Providers' web property.

493. Plaintiffs' and Class Members' computing devices derive value from their ability to facilitate communications with their Health Care Providers.

494. Google's past and ongoing trespasses deprive Plaintiffs and Class Members of the full value of using their computing devices and impair the quality and condition of those devices by converting them from tools for facilitating confidential communications into tools of Google's surveillance.

495. Google's trespass into Plaintiffs' and Class Members' computing devices resulted in harm to Plaintiffs and Class Members and caused the following damages:

- a. Nominal damages for trespass;
- b. Measurable loss of available storage and disk space on their communications and computing devices;
- c. Measurable loss of time caused by Google slowing the communications exchanged with the Health Care Providers;
- d. Measurable reduction in computing performance;
- e. Loss of quality and value of Plaintiffs' and Class Members' computing devices; and
- f. The total deprivation of Plaintiffs' and Class Members' use of their computing devices to communicate with Health Care Providers.

496. Google's repeated intrusions onto Plaintiffs' and Class Members' computing and communications devices via the placement of unauthorized Google Cookies disguised as belonging to the Plaintiffs' Health Care Providers, and its continuous acts to command the patients' and Class Members' computing and communications devices to use resources to re-direct

identifiers and communications content to Google and other third parties without consent, is evidence of Google's malicious disregard of Plaintiffs' and Class Members' property rights.

497. For Google's trespass, Plaintiffs and Class Members seek nominal damages, actual damages, general damages, unjust enrichment, punitive damages, and any other relief the Court deems just.

COUNT SEVEN
CALIFORNIA COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT
(On Behalf of All Classes)

498. Plaintiffs hereby incorporate the factual allegations set forth above by reference.

499. The California Comprehensive Computer Data Access and Fraud Act (CDAFA) was enacted to provide protection from "tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." Cal. Penal Code § 502(a).

500. The CDAFA affords a private right of action to owners of computers, systems, networks, programs, and data who suffer as a result of a violation of the Act. Cal. Penal Code § 502(e)(1).

501. The CDAFA imposes civil liability on anyone who:

a. Knowingly accesses and without permission alters, damages, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data. Cal. Penal Code § 502(c)(1);

b. Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network. Cal. Penal Code § 502(c)(2);

c. Knowingly and without permission uses or causes to be used computer services. Cal. Penal Code § 502(c)(3);

d. Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section. Cal. Penal Code § 502(c)(6);

e. Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network. Cal. Penal Code § 502(c)(7); and

f. Knowingly introduces any computer contaminant into any computer, computer system, or computer network. Cal. Penal Code § 502(c)(8).

502. “Computer services” under the CDAFA “includes, but is not limited to, computer time, data processing, or storage functions, or other uses of a computer, computer system, or computer network.” Cal. Penal Code § 502(b)(4).

503. “Computer network” is “any system that provides communications between one or more computer systems and input/output devices, including, but not limited to, display terminals, remote systems, mobile devices, and printers connected by telecommunication facilities.” Cal. Penal Code § 502(b)(2).

504. “Computer system” is “a device or collection of devices, including support devices...one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions, including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control.” Cal. Penal Code § 502(b)(5).

505. “Data” is defined as “a representation of information, knowledge, facts, concepts, computer software, or computer programs or instructions” that “may be in any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device.” Cal. Penal Code § 502(b)(8).

506. “Computer contaminant” means “any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, that are self-

replicating or self-propagating and are designed to contaminate other computer programs or computer data, consumer computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network.” Cal. Penal Code § 502(b)(12).

507. Google’s conduct, described herein, is in violation of Cal. Penal Code §§ 502(c)(1), (2), (3), (6), (7), and (8).

508. Plaintiffs and Class Members were the owners or lessees of the computers, computer systems, computer networks, and data described herein.

509. The Google Source Code and Google Cookies constitute “contaminants” under the CDAFA because they are designed to, and do, self-propagate to record and transmit data within users’ computers, computer systems, and computer networks that would not otherwise be transmitted in the normal operation of the computers, computer systems, and computer networks.

510. Google knowingly accessed, used, or caused to be used Plaintiffs’ and Class Members’ data, computers, computer services, and computer networks in that Google specifically designed the Google Source Code to surreptitiously place Google Cookies on patients’ computer browsers, which causes the devices’ data processing functions and networks to redirect Plaintiffs’ and Class Members’ Health Information to Google.

511. Google knowingly introduced Google Source Code into Plaintiffs’ and Class Members’ computers, computer systems, and computer networks and provided Health Care Providers with the means of accessing Plaintiffs’ and Class Members’ computers, computer systems, and computer networks in violation of the CDAFA by developing Google Source Code and encouraging and providing instructions to Health Care Providers on its use.

512. By depositing the Google Cookies disguised as first-party cookies and taking control of patient computing devices by commanding the computing devices to re-direct patient identifiers and communications content to Google and hundreds of third-parties in the middle of a patient’s communication with their Health Care Provider, Google has damaged those computing devices by reducing storage, disk space, and performance in a measurable way.

513. Plaintiffs' and Class Members' Health Information that Google redirects through the Google Source Code includes nonpublic information related to their communications with Health Care Providers.

514. Google makes use of Plaintiffs' and Class Members' Health Information to obtain money through advertising.

515. Google's use of Plaintiffs' and Class Members' Health Information is wrongful in that the use is prohibited by state and federal laws and Google's own policies, including but not limited to:

- a. The Federal wiretap Act, 18 U.S.C. §§ 2510 *et seq.*;
- b. CIPA;
- c. UCL;
- d. Google's Terms of Service and Google's Privacy Policy; and
- e. State law causes of actions for negligent misrepresentation, trespass, and invasion of privacy.

516. Google's use and access of Plaintiffs' and Class Members' data, computers, computer services, and computer networks, and Google's introduction of Google Source Code into Plaintiffs' and Class Members' computers, computer services, and computer networks is without permission because:

- a. Plaintiffs and Class Members never authorized Google to place Google cookies on their browser or otherwise access or use their data, computers, computer services, and computer networks;
- b. The Google Source Code was invisible to Plaintiffs and Class Members;
- c. Plaintiffs and Class Members were unaware that Google was using the Google Source Code to surreptitiously access and use their data, computers, computer services, and computer networks;
- d. It was impossible for Plaintiffs' and Class Members to opt-out of or prevent the functionality of the Google Source Code;

e. Google's own policies prohibit Google from accessing and using Plaintiffs' and Class Members' Health Information; and

f. Google circumvented technical and code-based barriers to access and use Plaintiffs' and Class Members' data, computers, computer services, and computer networks. The Google Source Code places Google cookies on Plaintiffs' and Class Members' computing devices, which are designed to disguise itself as a cookie from first-party Health Care Providers so that Google can circumvent cookie blockers and other technical barriers.

517. Plaintiffs' and Class Members' Health Information that Google accesses and uses is not publicly viewable and only became accessible to Google through Google's surreptitious and unauthorized placement of Google Cookies on Plaintiffs' and Class Members' computing devices.

518. Google's violations of the CDAFA have injured Plaintiffs and Class Members through damages and losses that include, but are not limited to:

a. The expenditure of time and resources to investigate Google's conduct, including the expenditure of time and resources to retain counsel to stop Google's conduct as applied to any future unavoidable communications that Plaintiffs and Class Members may be required to have via Health Care Provider web properties;

b. Google occupied storage space on their computers without authorization and without compensating Plaintiffs or Class Members' for such access;

c. Google caused the computers to work slower than they otherwise would in the absence of Google's actions and did not compensate Plaintiffs or Class Members' for such slowdowns;

d. Google used the computing resources of Plaintiffs and Class Members' computers without authorization and without compensating Plaintiffs or Class Members for use of such resources;

e. Google unjustly profited from the data taken from Plaintiffs' and Class Members' computer;

- f. The interruption or preclusion of Plaintiffs' and Class Members' ability to communicate with their Health Care Providers' web properties;
- g. A sense of violation and invasion based on past transmissions of information that Plaintiffs and Class Members had previously disclosed via their Health Care Provider web properties;
- h. A loss of trust in Plaintiffs' Health Care Providers' ability to maintain the privacy of their health/medical information;
- i. The diminution in value of Plaintiffs' and Class Members' Health Information; and
- j. Inability to use their computing devices for the purpose of communicating with their Health Care Providers.

519. As a result of Google's violations of the CDAFA, Plaintiffs and Class Members suffered damages including, but not limited to:

- a. The interruption or preclusion of their ability to communicate with their Health Care Providers on their Health Care Providers' web properties;
- b. The diminution in value of Plaintiffs' and Class Members' Health Information; and
- c. The inability of Plaintiffs to use their computing devices for the purpose of communication with their Health Care Providers.

520. Google's violations of the CDAFA were willful, fraudulent, or oppressive.

521. For Google's violations of the CDAFA, Plaintiffs and Class Members seek actual damages, general damages, unjust enrichment, punitive damages, appropriate injunctive or other equitable relief pursuant to Cal. Penal Code § 502(e)(1) and any other relief the Court deems just.

522. Pursuant to Cal. Penal Code § 502(e)(2), Plaintiffs and Class Members also ask the Court to award them their reasonable attorneys' fees.

COUNT EIGHT
BREACH OF EXPRESS CONTRACT
(On behalf of the Subclass of Google Account Holders)

523. Plaintiffs hereby incorporate the factual allegations set forth above by reference.

524. Plaintiffs in this subclass are Google Account Holders who exchanged communications with their Health Care Providers on their respective Health Care Providers' web properties where Google Source Code was placed, which resulted in the tracking and acquisition of their Health Information by Google.

525. An express contract was created between Google, on the one hand, and Plaintiffs and Class Members, on the other hand, whereby Google offered to provide Plaintiffs and Class Members with Google services (including, but not limited to, Gmail, YouTube, and YouTube TV) provided that Plaintiffs and Class Members agree to Google's Terms of Service and policy documents.

526. When a person signs up for a Google Account, Google requires users to state that they agree to the Google Terms of Service and Google Privacy Policy. As alleged above in Section IV-I, Google presents its Terms of Service one of five nested webpages on Google's Privacy & Terms webpage at the URL <https://policies.google.com/terms>, as a condition of opening, and subsequently of maintaining a Google Account.

527. The Google Terms of Service is binding on Google and Google Account Holders.

528. The Google Privacy Policy is binding on Google and Google Account Holders.

529. The Google Terms of Service and Google Privacy Policy are drafted exclusively by Google.

530. The Google Terms of Service and Privacy Policy are offered on a take-it-or-leave-it basis to consumers.

531. The Google Terms of Service expressly incorporates the Google Privacy Policy, declaring, "You also agree that our Privacy Policy applies to your use of our services." Google also incorporates and directs Google Account Holders to the contents of its Overview, Policies

Site/Technologies, FAQ, Google Product Privacy Guide, and Google Analytics Help webpages as well to numerous other hyperlinked policy documents.

532. Each of Google's statements on the webpages accessible from the Google Privacy & Terms webpage forms part of the express contract between Google and users of Google products and services, including Plaintiffs and Class Members.

533. Plaintiffs and Class Members did all they were required to do under the contracts.

534. Within the interconnected web of policies that form Google's contract, Google makes at least four promises that it has violated through its conduct alleged herein:

535. Promise 1: Google committed that it had established and enforces rules of conduct that prohibit violating laws and privacy rights through use of Google services.

536. Promise 2: Google committed to collect only health information that users choose to provide.

537. Promise 3: Google committed, categorically, not to use information pertaining to health for advertising or permit others to do so.

538. Promise 4: Google committed to use the information it obtains from other websites and applications to enforce the rules of conduct.

539. With respect to patients who are Google Account Holders, the promises operate as contractually binding terms between Google and Google Account Holders because Google requires that all Google Account Holders expressly agree to these contracts of adhesion upon signing up to be a Google Account Holder.

540. Google materially breached Promise 1 by failing to respect the privacy rights of Plaintiffs and Class Members with its own acquisition and use of their Health Information, and by encouraging Health Care Providers to use Google Source Code in violation of those rights, rather than terminating their use of Google services upon learning of the violations.

541. Google materially breached Promise 2 by collecting the Health Information of Plaintiffs and Class Members through the automatic operation of Google Source Code when

Plaintiffs and Class Members did not choose to provide it. The Health Information that Google obtained without Plaintiffs' consent in material breach of its agreement with users includes:

- a. Patient identifiers including, but not limited to, email addresses, IP addresses, persistent cookie identifiers, device identifiers, and browser fingerprint information;
- b. the date and time of patient registrations for their Health Care Providers' patient portals;
- c. log-in and log-out times for their Health Care Providers' patient portals;
- d. the contents of communications that patients exchange inside their Health Care Providers' patient portals;
- e. the contents of communications relating to medical appointments;
- f. the contents of communications relating to prescription drugs;
- g. the contents of communications relating to health insurance; and,
- h. the user's status as a patient, subscriber, and/or user of their Health Care Provider.

542. Google materially breached Promise 3 by using and permitting Health Information to be used to show personalized ads, including by using Health Information collected through Google Source Code to develop algorithms and other processes for ad targeting even in cases where that Health Information was not used directly to target a particular advertisement. Google's breach of its promise not to use Health Information or permit advertisers to use Health Information occurs through Google Analytics, Google Ads, Google Display Ads, and YouTube, both directly on Google owned-and-operated properties (including Google.com, YouTube) and on non-Google web properties where Google advertising tools are deployed. Google maintains developer pages instructing advertisers on how to breach the specific promises relating to Health Information. Google can and does link the Health Information collected, including the Health Information collected and re-directed to Google Analytics, across its various systems and products to be used in its advertising services. Google does not take action to stop, suspend, or discipline itself or a

Health Care Provider for unlawful conduct (which under Google's own definition constitutes "egregious conduct") involving Google's collection of Health Information from Health Care Providers and, it does not "err on the side caution" in enforcing these commitments but, instead, creates a system that facilitates the use and showing of targeted advertising based on sensitive categories, like health.

543. Google breached Promise 4 by using Health Information and other data transmitted by Healthcare Provider websites for advertising purposes in violation of privacy rights, instead of using that data to protect against the violation of privacy rights. Google does not use its systems or the data transmitted therein to require Health Care Providers to comply with applicable law, to respect privacy rights, or to refrain from engaging in misleading or fraudulent conduct in the unlawful tracking, collection and disclosure to Google of patients' Health Information.

544. Google's breach of these promises caused Plaintiffs and Class Members the following damages:

- a. Nominal damages for breach of contract;
- b. General damages for invasion of their privacy rights in an amount to be determined by a jury without reference to specific pecuniary harm;
- c. Sensitive and confidential information including patient status and appointments that Plaintiffs and Class Members intended to remain private are no longer private;
- d. Google eroded the essential confidential nature of the patient-provider relationship;
- e. Google took something of value from Plaintiffs and Class Members and derived benefits therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without sharing the benefit of such value; and,
- f. Benefit of the bargain damages in that Google's contract stated that payment for the service would consist of a more limited set of collection of personal information than that which Google actually charged.

COUNT NINE
BREACH OF IMPLIED CONTRACT
(On behalf of All Classes)

545. Plaintiffs hereby incorporate the factual allegations set forth above by reference.

546. To the extent that Google's Terms of Service and policy documents are not express contracts and/or do not contain terms incorporated by reference within express contracts, Plaintiffs allege, in the alternative, that they set forth the agreed upon terms of implied contracts.

547. Plaintiffs and all Class Members are individuals who interacted with Google's services. Interacting with Google's services imposes certain obligations. An implied contract was created between Google, on the one hand, and Plaintiffs and Class Members, on the other hand, whereby Google offered to provide Plaintiffs and Class Members the ability to interact with Google services (including, but not limited to, Gmail, YouTube, and YouTube TV) under the conditions set forth in Google's Terms of Service and other policy documents alleged and described herein. Plaintiffs and Class Members accepted these conditions through their conduct in interacting with Google's services, and Google accepted these conditions, including its obligations to abide by its Promises 1 – 4, by its conduct in offering and providing its services to Plaintiffs and Class members.

Mutual Assent

548. Such implied contract was created by virtue of the conduct of the parties, as well as the surrounding circumstances, including, but not limited to:

- a. Google's express promises, alleged and described above;
- b. Federal, State, and common law protections regarding Health Information; and
- c. Plaintiffs' and Class Members' reasonable expectation of privacy over their Health Information.

549. Google knew, or had reason to know, that Plaintiffs and Class Members would interpret the parties' conduct as an agreement that Google would not collect, use, or monetize

Plaintiffs' and Class Members' Health Information when they interacted with Google services without their authorization.

Consideration

550. Google does not provide its services without receiving anything from Plaintiffs and Class Members in return. To the contrary, Plaintiffs' and Class Members' interaction with Google's services confers significant benefit upon Google—a benefit to which Google is not entitled—money.

551. Specifically, when Plaintiffs and Class Members interact with Google's services, Google is able to collect information, including Health Information, about Plaintiffs and Class Members. Google monetizes users' Health Information by serving personalized ads to users, as described above.

552. In fact, the vast majority of the money Google makes comes from advertising. In 2022 alone, Google generated over \$224 billion from advertising.

Performance

553. Plaintiffs performed under the implied contract by using and interacting with Google's services.

Google's Breach of the Implied Contract

554. Google materially breached its implied contract with Plaintiffs and Class Members by collecting, using, and monetizing their Health Information when they interacted with Google services without authorization.

555. The Health Information Google collects is not publicly accessible click or browsing data.

556. Nevertheless, information that Plaintiffs and Class Members reasonably thought was private and secure was being collected, used, and monetized by Google.

557. Plaintiffs and Class Members did not authorize Google to collect, use, or monetize their Health Information.

558. Google has failed and refused to cure these breaches and continues to collect, use, and monetize Plaintiffs' and Class Members' Health Information.

559. Google's breach caused Plaintiffs and Class Members the following damages:

- a. Nominal damages for each breach of contract;
- b. General damages for invasion of their rights in an amount to be determined by a jury without reference to specific pecuniary harm;
- c. Sensitive and confidential information that Plaintiffs and Class Members intended to remain private is no longer private;
- d. Google took something of value from Plaintiffs and Class Members and derived benefit therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without sharing the benefit of such value;
- e. Google's actions diminished the value of Plaintiffs' and Class Members' Health Information;
- f. Google's actions violated the property rights Plaintiffs and Class Members enjoy in their private communications; and
- g. Google's actions violated the property rights Plaintiffs and Class Members enjoy in their Health Information.

560. Plaintiffs and Class Members also seek costs on this claim to the extent allowable.

COUNT TEN
GOOD FAITH AND FAIR DEALING
(On behalf of the Subclass of Google Account Holders)

561. Plaintiffs hereby incorporate the factual allegations set forth above by reference.

562. A valid contract exists between Plaintiffs and Google.

563. The contract specifies that California law governs the parties' relationship.

564. Google prevented Plaintiffs and Class Members from receiving the full benefit of the contract by intercepting their Health Information.

565. By doing so, Google abused its power to define terms of the contract, including but not limited to:

- a. Google's effort to limit the meaning of "Health Information" to something that is not consistent with what any reasonable person would understand and directly contrary to federal and state laws, as well as patients' reasonable expectations of privacy;
- b. Google's effort to change the meaning of the term "personally identifiable information" in its statements to publishers and advertisers in a way that is directly contrary to (1) the plain English meaning of the term "identifyable;" (2) federal and state law; and (3) the definitions of "personal information" under Google's Privacy Policy and California law—adopted by Google's Privacy Policy; and,
- c. Google's effort to interpret "personalized advertising" to exclude remarketing, conversion tracking, and contextual health information ads on Health Care Provider properties based on Health Information and communications of Plaintiffs and Class Members at those Health Care Provider properties

566. By doing so, Google did not act fairly and in good faith.

567. Google's breach caused Plaintiffs and Class Members the following damages:

- a. Nominal damages for breach of contract;
- b. General damages for invasion of their privacy rights in an amount to be determined by a jury without reference to specific pecuniary harm;
- c. Sensitive and confidential information including patient status and appointments that Plaintiffs and Class Members intended to remain private are no longer private;
- d. Google eroded the essential confidential nature of the patient-provider relationship;
- e. Google took something of value from Plaintiffs and Class Members and derived benefits therefrom without Plaintiffs' and Class Members' knowledge or informed consent and without sharing the benefit of such value; and

f. Benefit of the bargain damages in that Google's contract stated that payment for the service would consist of a more limited set of collection of personal information than that which Google actually charged.

COUNT ELEVEN
UNJUST ENRICHMENT UNDER CALIFORNIA COMMON LAW
(On Behalf of All Classes)

568. Plaintiffs hereby incorporate the factual allegations set forth above by reference.

569. California common law on unjust enrichment is applicable for all members of the U.S. Health User Class.

570. Google has wrongfully and unlawfully trafficked in the named Plaintiffs' and the Class Members' Health Information and other personal data without their consent for substantial profits.

571. Plaintiffs' and Class Members' Health Information and data have conferred an economic benefit on Google.

572. Google has been unjustly enriched at the expense of Plaintiffs and Class Members, and the company has unjustly retained the benefits of its unlawful and wrongful conduct.

573. The remedies available to Plaintiffs' and Class Members are inadequate to compensate them for the injuries they have suffered as a result of Google's conduct. Thus, it would be inequitable and unjust for Google to be permitted to retain any of the unlawful proceeds resulting from its unlawful and wrongful conduct.

574. Plaintiffs and Class Members accordingly are entitled to equitable relief including restitution and disgorgement of all revenues, earnings, and profits that Google obtained as a result of its unlawful and wrongful conduct.

575. When a defendant is unjustly enriched at the expense of a plaintiff, the plaintiff may recover the amount of the defendant's unjust enrichment even if plaintiff suffered no corresponding loss, and plaintiff is entitled to recovery upon a showing of a mere violation of legally protected rights that enriched a defendant. Google has been unjustly enriched by virtue of its violations of Plaintiffs' and Class Members' legally protected rights to privacy as alleged

herein, entitling Plaintiffs and Class Members to restitution of Google's enrichment. “[T]he consecrated formula ‘at the expense of another’ can also mean ‘in violation of the other’s legally protected rights,’ without the need to show that the claimant has suffered a loss.” Restatement (Third) of Restitution § 1, cmt. a.

576. The elements for a claim of unjust enrichment are (1) receipt of a benefit and (2) unjust retention of the benefit at the expense of another. The doctrine applies where plaintiffs, while having no enforceable contract, nonetheless have conferred a benefit on defendant which defendant has knowingly accepted under circumstances that make it inequitable for the defendant to retain the benefit without paying for its value.

577. It is a longstanding principle of law embodied in the Restatement (Third) of Restitution and Unjust Enrichment (2011) that a person who is unjustly enriched at the expense of another may be liable for the amount of unjust enrichment even if the defendant’s actions caused the plaintiff no corresponding loss. Where “a benefit has been received by the defendant but the plaintiff has not suffered a corresponding loss or, in some cases, any loss, but nevertheless the enrichment of the defendant would be unjust ... [t]he defendant may be under a duty to give to the plaintiff the amount by which [the defendant] has been enriched.” Rest., Restitution, § 1, com. e.

578. The comments to the Restatement (Third) explicitly recognize that an independent claim for unjust enrichment may be predicated on a privacy tort. Restatement (Third) of Restitution and Unjust Enrichment § 44 cmt. b (“Profitable interference with other protected interests, such as the claimant’s right of privacy, gives rise to a claim under § 44 if the benefit to the defendant is susceptible of measurement”).

579. Moreover, the Restatement recognizes that in the context of a privacy violation, the claimant need not be in direct privity with the wrongdoer, and likewise, California law imposes no requirement of privity to make out an unjust enrichment claim. The Restatement comments provide the following illustrative example:

10. On going out of business, Local Pharmacy sells Customers' prescription records and accompanying medical information to National Chain. In connection with the sale, Local Pharmacy agrees not to inform Customers of the pending disclosure of

their records; the object of this provision is to allow National Chain to communicate with Customers once their files have been transferred. Because it gives Customers no opportunity to object to the disclosure of confidential information, the transaction between Local Pharmacy and National Chain is both a violation of Customers' protected right of privacy in their prescription records and a deceptive marketing practice under local law. By the rule of this section, Customers have a claim against Local Pharmacy for the proceeds of the sale of their confidential information, *and a claim against National Chain for the additional profits it derived from the unlawful transaction.*

Id. § 44 cmt. b, illus. 10 (emphasis added).

580. Because “[a] person is not permitted to profit by his own wrong,” *id.* § 3, “[g]ains realized by misappropriation, or otherwise in violation of another’s legally protected rights, must be given up to the person whose rights have been violated.” *Id.* ch. 5, introductory note. These principles are deeply ingrained in California law. California courts have long recognized a common law claim based on unjust enrichment. In determining the remedy for such claims, California courts apply principles found in the Restatement.

581. The public policy of California does not permit one to “take advantage of his own wrong” regardless of whether the other party suffers actual damage. Where the defendant has been unjustly enriched but the plaintiff has not proven any monetary loss, the proper remedy is for the defendant to disgorge those ill-gotten gains. A defendant acting in conscious disregard of the rights of another should be required to disgorge all profit because disgorgement both benefits the injured parties and deters the perpetrator from committing the same unlawful actions again. Without this result, there would be an insufficient deterrent to improper conduct that is more profitable than lawful conduct. “Restitution requires full disgorgement of profit by a conscious wrongdoer, not just because of the moral judgment implicit in the rule of this section, but because any lesser liability would provide an inadequate incentive to lawful behavior.” Restatement (Third) of Restitution and Unjust Enrichment § 3, cmt. b.

582. The unauthorized use of Plaintiffs’ and Class Members’ information for profit entitles them to profits unjustly earned. That is so, moreover, regardless of whether Plaintiffs and Class Members planned to sell their data or whether the individual’s data is made less valuable, and regardless of whether Plaintiffs and Class Members were in privity with Google.

583. Google has unjustly profited from using private Health Information to third parties without Plaintiffs' and Class Members' knowledge or consent.

584. A portion—but not all—of the unjust enrichment Google obtained was through the Plaintiffs' and Class Members' use of Health Care Provider web properties, which constitutes an invasion of privacy. Moreover, the access Plaintiffs and Class Members received to those web properties does not defeat their unjust enrichment claim because:

a. As described above, Plaintiffs were not aware of Google's conduct while communicating with their Health Care Providers on the Health Care Providers' web properties, and did not and could not consent to that conduct. Had Plaintiffs known of Google's conduct, Plaintiffs would not have visited those websites or, if such visits were unavoidable, would have taken additional precautions to avoid being tracked and profiled by Google. Google's conduct with respect to tracking Plaintiffs' conduct on any particular web properties cannot be viewed in isolation—the aggregation, compilation, analysis, and sale of that extensive information about Plaintiffs' habits—and personal and private medical communications—violates Plaintiffs' California Constitutional and common law rights. Moreover, the fruits of Google's illegal wiretapping of Plaintiffs' communications with Health Care Provider web properties, in violation of criminal statutes, also contributed to Google's enrichment. Google's enrichment through violation of criminal wiretapping statutes is inherently unjust.

b. Plaintiffs were not aware of and did not consent to the collection of their Health Information by Google, which is independent of their visit to any web property. Google was unjustly enriched by the acquisition and monetization of Plaintiffs' private Health Information.

585. Plaintiffs did not provide authorization for the use of their information, nor did Google provide them with control over its use to produce revenue. This unauthorized use of their information for profit entitles Plaintiffs to profits unjustly earned.

586. Plaintiffs' aggregate Health Information carries financial value. Google was unjustly enriched by aggregating Plaintiffs' personal and sensitive Health Information and monetizing that data to obtain financial gain.

587. The portion of Google's revenue attributable to Google's wrongful conduct described herein is susceptible of measurement and can be determined through discovery.

588. It would be unjust and inequitable to allow Google to profit from its violation of the Plaintiffs' and Class Members' Constitutional, common law, and statutory rights as described herein. Google's conduct in collecting and using Plaintiffs' and Class Members' private Health Information is conduct that was specifically singled out for disapprobation by the voters of California in amending the California Constitution. Google's conduct is highly offensive to a reasonable person, and as such, regardless of whether Plaintiffs and Class Members received anything of value from the web properties they visited, Google's profiting from its collection and use of their data violates California public policy and goes well beyond acceptable social norms.

589. Google was aware of the benefit conferred by Plaintiffs and Class Members. Indeed, Google Analytics, Google Ads, Google Display Ads, and YouTube are premised on the sale of such data to third parties. Google acted in conscious disregard of the rights of Plaintiffs and Class Members and should be required to disgorge all profit obtained therefrom to deter Google and others from committing the same unlawful actions again.

COUNT TWELVE
CONVERSION
(On Behalf of All Classes)

590. Plaintiffs hereby incorporate the factual allegations set forth above by reference.

591. Property is the right of any person to possess, use, enjoy, or dispose of a thing, including intangible things like data and communications.

592. The Health Information at issue here is property under California law.

593. Plaintiffs and Class members have an ownership and property interest in their own Health Information as they would any other property.

594. Through its Source Code, Google wrongfully obtained, stored, disposed, used, and otherwise exercised dominion and control over Plaintiffs' and Class Members' Health Information, including for its own commercial purposes.

595. The use of Google's Source Code to obtain, store, dispose, use, and otherwise exercise dominion and control over Plaintiffs' and Class Members' Health Information was a wrongful act because it was done intentionally in a surreptitious manner without Plaintiffs' and Class Members' knowledge or consent.

596. As a result of Google's conduct, it wrongfully exercised control over Plaintiffs' and Class Members' property and has not returned it, depriving Plaintiffs and Class Members of their property interest. Indeed, the Health Information property Google converted remains in its systems to this day and continues to be used for its commercial purposes.

597. There is no excuse or justification for Google's conversion of Plaintiffs' and Class Members' Health Information.

598. Plaintiffs and Class Members have been damaged as a result of Google's unlawful conversion of their property. Google's conversion of individuals' Health Information without authorization has caused harm to Plaintiffs' and Class members' protected property interest in this information. Plaintiffs are entitled to a disgorgement and/or restitution damages for the value of their stolen property, as well as any unjustly earned profits as a result of Google's conversion.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that this Court:

A. Certify the proposed Classes, designating Plaintiffs as the named representatives of the Class, and designating the undersigned as Class Counsel;

- B. Permanently restrain Defendant, and its officers, agents, servants, employees and attorneys, from using Google Source Code to track, obtain and use Plaintiffs' and Class Members' Health Information;
- C. Award compensatory damages, including statutory damages where available, to Plaintiffs and the Class against Google for all damages sustained as a result of Google's wrongdoing, in an amount to be proven at trial, including interest thereon;
- D. Award punitive damages on the causes of action that allow for them and in an amount that will deter Google and others from like conduct;
- E. Enter judgment in favor of Plaintiffs and the members of the Class against Google awarding unjust enrichment and/or restitution of Google's ill-gotten gains, revenues, earnings, or profits that it derived, in whole or in part, from its unlawful collection and use of Class Members' personal data, in an amount according to proof at trial;
- F. Award attorneys' fees and costs, as allowed by law including, but not limited to, California Code of Civil Procedure section 1021.5;
- G. Award pre-judgment and post-judgment interest, as provided by law; and
- H. For such other, further, and different relief as the Court deems proper under the circumstances.

Dated: November 16, 2023

SIMMONS HANLY CONROY LLC

/s/ Jay Barnes

Jason 'Jay' Barnes

Jason 'Jay' Barnes (admitted *pro hac vice*)

jaybarnes@simmonsfirm.com

Eric Johnson (admitted *pro hac vice*)

ejohnson@simmonsfirm.com

An Truong (admitted *pro hac vice*)

atruong@simmonsfirm.com

112 Madison Avenue, 7th Floor

New York, NY 10016

Tel.: 212-784-6400

Fax: 212-213-5949

Dated: November 16, 2023

LOWEY DANNENBERG, P.C.

/s/ Christian Levis

Christian Levis

Christian Levis (admitted *pro hac vice*)
clevis@lowey.com

Amanda Fiorilla (admitted *pro hac vice*)
afiorilla@lowey.com

44 South Broadway, Suite 1100

White Plains, NY 10601

Tel: (914) 997-0500

Fax: (914) 997-0035

KIESEL LAW LLP

Jeffrey A. Koncious, State Bar No. 189803
koncious@kiesel.law

Paul R. Kiesel, State Bar No. 119854
kiesel@kiesel.law

Nicole Ramirez, State Bar No. 279017
ramirez@kiesel.law

8648 Wilshire Boulevard

Beverly Hills, CA 90211-2910

Tel: 310-854-4444

Fax: 310-854-0812

**LIEFF CABRASER HEIMANN
& BERNSTEIN, LLP**

Michael W. Sobol (State Bar No. 194857)
msobel@lchb.com

Melissa Gardner (State Bar No. 289096)
mgardner@lchb.com

Jallé H. Dafa (State Bar No. 290637)
jdfa@lchb.com

275 Battery Street, 29th Floor
San Francisco, CA 94111-3339

Tel: 415 956-1000

Fax: 415-956-1008

Douglas Cuthbertson (admitted *pro hac vice*)
dcuthbertson@lchb.com

250 Hudson Street, 8th Floor
New York, NY 10013

Tel: 212 355-9500

Fax: 212-355-9592

SCOTT+SCOTT ATTORNEYS AT LAW LLP

Hal D. Cunningham (Bar No. 243048)

hcunningham@scott-scott.com

Sean Russell (Bar No. 308962)

srussell@scott-scott.com

600 W. Broadway, Suite 3300

San Diego, CA 92101

Tel: (619) 233-4565

Fax: (619) 233-0508

Joseph P. Guglielmo (admitted *pro hac vice*)

jguglielmo@scott-scott.com

Ethan Binder (admitted *pro hac vice*)

ebinder@scott-scott.com

230 Park Ave., 17th Floor

New York, NY 10169

Telephone: (212) 223-6444

Facsimile: (212) 223-6334

Attorneys for Plaintiffs and the Proposed Class

IX. DEMAND FOR JURY TRIAL

Pursuant to F.R.C.P. Rule 38, Plaintiffs, on behalf of themselves and the Classes, demand a trial by jury of any and all issues in this action so triable of right.

Dated: November 16, 2023

SIMMONS HANLY CONROY LLC

/s/ Jay Barnes

Jason 'Jay' Barnes

Jason 'Jay' Barnes (admitted *pro hac vice*)

jaybarnes@simmonsfirm.com

Eric Johnson (admitted *pro hac vice*)

ejohnson@simmonsfirm.com

An Truong (admitted *pro hac vice*)

atruong@simmonsfirm.com

112 Madison Avenue, 7th Floor

New York, NY 10016

Tel.: 212-784-6400

Fax: 212-213-5949

Dated: November 16, 2023

LOWEY DANNENBERG, P.C.

/s/ Christian Levis

Christian Levis

Christian Levis (admitted *pro hac vice*)

clevis@lowey.com

Amanda Fiorilla (admitted *pro hac vice*)

afiorilla@lowey.com

44 South Broadway, Suite 1100

White Plains, NY 10601

Tel: (914) 997-0500

Fax: (914) 997-0035

KIESEL LAW LLP

Jeffrey A. Koncious, State Bar No. 189803

koncious@kiesel.law

Paul R. Kiesel, State Bar No. 119854

kiezel@kiesel.law

Nicole Ramirez, State Bar No. 279017

ramirez@kiesel.law

8648 Wilshire Boulevard

Beverly Hills, CA 90211-2910

Tel: 310-854-4444

Fax: 310-854-0812

**LIEFF CABRASER HEIMANN
& BERNSTEIN, LLP**

Michael W. Sobol (State Bar No. 194857)

msobol@lchb.com

Melissa Gardner (State Bar No. 289096)

mgardner@lchb.com

Jallé H. Dafa (State Bar No. 290637)

jdfa@lchb.com

275 Battery Street, 29th Floor

San Francisco, CA 94111-3339

Tel: 415 956-1000

Fax: 415-956-1008

Douglas Cuthbertson (admitted *pro hac vice*)

dcuthbertson@lchb.com

250 Hudson Street, 8th Floor

New York, NY 10013

Tel: 212 355-9500

Fax: 212-355-9592

SCOTT+SCOTT ATTORNEYS AT LAW LLP

Hal D. Cunningham (Bar No. 243048)

hcunningham@scott-scott.com

Sean Russell (Bar No. 308962)

srussell@scott-scott.com

600 W. Broadway, Suite 3300

San Diego, CA 92101

Tel: (619) 233-4565

Fax: (619) 233-0508

Joseph P. Guglielmo (admitted *pro hac vice*)

jguglielmo@scott-scott.com

Ethan Binder (admitted *pro hac vice*)

ebinder@scott-scott.com

230 Park Ave., 17th Floor

New York, NY 10169

Telephone: (212) 223-6444

Facsimile: (212) 223-6334

Attorneys for Plaintiffs and the Proposed Class

ATTESTATION

Pursuant to Civil Local Rule 5-1(h)(3), I hereby attest that all signatories listed, and on whose behalf the filing is submitted, concur in the filing's content and have authorized the filing.

Dated: November 16, 2023

/s/ Jeffrey A. Koncius
Jeffrey A. Koncius

APPENDIX A: INDEX OF EXHIBITS

No.	Name	URL (last visited Nov. 13, 2023)
Exhibit 1	<i>HIPAA and Google Analytics</i> , GOOGLE ANALYTICS HELP (print-friendly reproduction)	https://support.google.com/analytics/answer/13297105
Exhibit 2	<i>Analytics</i> , GOOGLE MARKETING PLATFORM	https://marketingplatform.google.com/about/analytics/
Exhibit 3	<i>Analytics 360</i> , GOOGLE MARKETING PLATFORM	https://marketingplatform.google.com/about/analytics-360/features/#integrations
Exhibit 4	<i>Set up your Google tag</i> , GOOGLE ANALYTICS HELP (print-friendly reproduction)	https://support.google.com/analytics/answer/12002338
Exhibit 5	<i>Analytics for Firebase</i> , GOOGLE FIREBASE DOCUMENTATION (print-friendly reproduction)	https://firebase.google.com/docs/analytics
Exhibit 6	<i>Diagram within Safeguarding Your Data</i> , GOOGLE ANALYTICS HELP	https://storage.googleapis.com/support-kms-prod/473DwRsuvOOYAIYdctqvnQp1pn2BLXRqSEmV
Exhibit 7	<i>How Google Analytics Collects Data</i> , ANALYTICS MARKET	https://www.analyticsmarket.com/blog/how-google-analytics-collects-data/
Exhibit 8	<i>Measurement Protocol Parameter Reference</i> , GOOGLE FOR DEVELOPERS/ANALYTICS	https://developers.google.com/analytics/devguides/collection/protocol/v1/parameters
Exhibit 9	<i>Set up and install Tag Manager</i> , GOOGLE TAG MANAGER HELP (print-friendly reproduction)	https://support.google.com/tagmanager/answer/6103696
Exhibit 10	<i>Measurement Protocol Reference</i> , GOOGLE FOR DEVELOPERS/ANALYTICS (print-friendly reproduction)	https://developers.google.com/analytics/devguides/collection/protocol/v1/reference
Exhibit 11	<i>About the Google tag</i> , GOOGLE FOR DEVELOPERS/TAG PLATFORM (print-friendly reproduction)	https://developers.google.com/tag-platform/gtagjs
Exhibit 12	<i>Tag Manager and the Google Tag</i> , GOOGLE TAG MANAGER HELP (print-friendly reproduction)	https://support.google.com/tagmanager/answer/7582054
Exhibit 13	<i>About Customer Match</i> , GOOGLE ADS HELP (print-friendly reproduction)	https://support.google.com/google-ads/answer/6379332
Exhibit 14	<i>How Google Uses Customer Match Data</i> , GOOGLE ADS HELP (print-friendly reproduction)	https://support.google.com/google-ads/answer/6334160
Exhibit 15	<i>Create a Customer List</i> , GOOGLE ADS HELP (print-friendly reproduction)	https://support.google.com/google-ads/answer/6276125
Exhibit 16	<i>Use the Google Tag for Google Ads Conversion Tracking</i> , GOOGLE ADS HELP (print-friendly reproduction)	https://support.google.com/google-ads/answer/7548399
Exhibit 17	<i>About Your Data Segments for Search Ads</i> , GOOGLE ADS HELP (print-friendly reproduction)	https://support.google.com/google-ads/answer/2701222
Exhibit 18	<i>About Your Data Segments</i> , GOOGLE ADS HELP (print-friendly reproduction)	https://support.google.com/google-ads/answer/2453998

Exhibit 19	<i>Tag Your Website Using Google Ads</i> , GOOGLE ADS HELP (print-friendly reproduction)	https://support.google.com/google-ads/answer/2476688
Exhibit 20	<i>Prevent Ads from Displaying to Members of Google Ads Remarketing Lists: Create a Negative Remarketing Target</i> , GOOGLE SEARCH ADS 360 HELP (print-friendly reproduction)	https://support.google.com/searchads/answer/6108309
Exhibit 21	<i>Set Up Remarketing Lists for Display Ads</i> , GOOGLE SEARCH ADS 360 HELP (print-friendly reproduction)	https://support.google.com/searchads/answer/7201620
Exhibit 22	<i>Use Your Data Segments to Advertise on YouTube</i> , GOOGLE ADS HELP (print-friendly reproduction)	https://support.google.com/google-ads/answer/7181409
Exhibit 23	<i>Remarketing Lists for Search Ads with Analytics</i> , GOOGLE ANALYTICS HELP (print-friendly reproduction)	https://support.google.com/analytics/answer/6212951
Exhibit 24	<i>How Placements and Keywords Work Together</i> , GOOGLE ADS HELP (archived Jan. 24, 2023, print-friendly reproduction)	http://web.archive.org/web/20230124150222/https://support.google.com/google-ads/answer/2580292
Exhibit 25	<i>Contextual Targeting</i> , GOOGLE ADS HELP (print-friendly reproduction)	https://support.google.com/google-ads/answer/1726458
Exhibit 26	<i>Google Display Network and YouTube on Computers, Mobile Devices, and Tablets</i> , GOOGLE ADS HELP (print-friendly reproduction)	https://support.google.com/google-ads/answer/2740623
Exhibit 27	<i>About Remarketing Audiences in Analytics</i> , GOOGLE ANALYTICS HELP (print-friendly reproduction)	https://support.google.com/analytics/answer/2611268
Exhibit 28	<i>Link Google Ads to Firebase</i> , GOOGLE FIREBASE HELP (print-friendly reproduction)	https://support.google.com/firebase/answer/6383833
Exhibit 29	<i>Reporting Identity</i> , GOOGLE ANALYTICS HELP (print-friendly reproduction)	https://support.google.com/analytics/answer/10976610
Exhibit 30	<i>Organizing Information - How Google Search Works</i> , GOOGLE SEARCH (print-friendly reproduction)	https://www.google.com/search/howsearchworks/how-search-works/organizing-information
Exhibit 31	<i>In-depth Guide to How Google Search Works</i> , GOOGLE SEARCH CENTRAL (print-friendly reproduction)	https://developers.google.com/search/docs/fundamentals/how-search-works
Exhibit 32	<i>Privacy in Health Care: Code of Medical Ethics Opinion 3.1.1</i> , AM. MED. ASS'N	https://code-medical-ethics.ama-assn.org/sites/default/files/2022-08/3.1.1.pdf
Exhibit 33	<i>Access to Medical Records by Data Collection Companies: Opinion 3.2.4</i> , AM. MED. ASS'N	https://code-medical-ethics.ama-assn.org/sites/default/files/2022-08/3.2.4.pdf
Exhibit 34	<i>Confidentiality & Electronic Medical Records: Code of Medical Ethics Opinion 3.3.2</i> , AM. MED. ASS'N	https://code-medical-ethics.ama-assn.org/sites/default/files/2022-08/3.3.2.pdf

Exhibit 35	<i>Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the HIPAA Privacy Rule</i> , U.S. DEP'T OF HEALTH AND HUM. SERV. (Excerpts; pp.1-9 [Section 1]; Glossary)	https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/D-e-identification/hhs_deid_guidance.pdf
Exhibit 36	<i>Marketing</i> , U.S. DEP'T OF HEALTH AND HUM. SERV.	https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf
Exhibit 37	<i>Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates</i> , U.S. DEP'T OF HEALTH AND HUM. SERV.	https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html
Exhibit 38	<i>Elisa Jillson, Protecting the Privacy of Health Information: A Baker's Dozen Takeaways from FTC Cases</i> , FED. TRADE COMM'N BUSINESS BLOG (print-friendly reproduction)	https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases
Exhibit 39	<i>FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies</i> , FED. TRADE COMM'N (print-friendly reproduction)	https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking
Exhibit 40	<i>HHS and FTC Joint Letter to Third Party Trackers</i> , FED. TRADE COMM'N	https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf
Exhibit 41	<i>Terms of Service</i> , GOOGLE PRIVACY & TERMS (downloadable PDF)	https://policies.google.com/terms
Exhibit 42	<i>Privacy Policy</i> , GOOGLE PRIVACY & TERMS (Dec. 15, 2022) (downloadable PDF)	https://policies.google.com/privacy/archive/20221215
Exhibit 43	<i>Overview</i> , GOOGLE PRIVACY & TERMS (print-friendly reproduction)	https://policies.google.com/
Exhibit 44	<i>Google Product Privacy Guide</i> , GOOGLE PRIVACY & TERMS (partial screenshot)	https://policies.google.com/technologies/product-privacy
Exhibit 45	<i>List of Services & Specific Additional Terms</i> , GOOGLE PRIVACY & TERMS	https://policies.google.com/terms/service-specific
Exhibit 46	<i>Report Abuse or Legal Issue</i> , GOOGLE GROUPS HELP (print-friendly reproduction)	https://support.google.com/groups/answer/81275
Exhibit 47	<i>Personalized Advertising</i> , GOOGLE ADVERTISING POLICIES HELP (print-friendly reproduction)	https://support.google.com/adspolicy/answer/143465
Exhibit 48	<i>What Happens if You Violate Our Policies</i> , GOOGLE ADVERTISING POLICIES HELP (print-friendly reproduction)	https://support.google.com/adspolicy/answer/7187501

Exhibit 49	<i>Legal Requirements</i> , GOOGLE ADVERTISING POLICIES HELP (archived Mar. 6, 2023)	https://web.archive.org/web/20230306142755/https://support.google.com/adspolicy/answer/6023676
Exhibit 50	<i>Safeguarding Your Data</i> , GOOGLE ANALYTICS HELP (print-friendly reproduction)	https://support.google.com/analytics/answer/600424
Exhibit 51	<i>Technologies: Advertising: How Google uses information from sites or apps that use our services</i> , GOOGLE PRIVACY & TERMS (print-friendly reproduction)	https://policies.google.com/technologies/partner-sites
Exhibit 52	<i>Healthcare and Medicines</i> , GOOGLE ADVERTISING POLICIES HELP (archived Feb. 3, 2023, print-friendly reproduction; Excerpts pp. 1-19)	https://web.archive.org/web/20230203100832/https://support.google.com/adspolicy/answer/176031
Exhibit 53	<i>Introducing the Next Generation of Analytics</i> , Google Analytics 4, GOOGLE ANALYTICS HELP (print-friendly reproduction)	https://support.google.com/analytics/answer/13297105
Exhibit 54	<i>Best Practices to Avoid Sending Personally Identifiable Information (PII)</i> , GOOGLE AD MANAGER HELP (print-friendly reproduction)	https://marketingplatform.google.com/about/analytics/
Exhibit 55	<i>False Positives and Personally Identifiable Information (PII)</i> , GOOGLE AD MANAGER HELP (print-friendly reproduction)	https://marketingplatform.google.com/about/analytics-360/features/#integrations